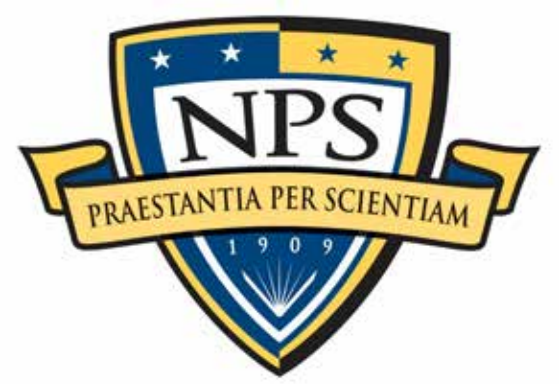
2020-12

DRONE AMERICA: THE END OF PRIVACY?

Farias, Richard T.

Monterey, CA; Naval Postgraduate School



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DRONE AMERICA: THE END OF PRIVACY?

by

Richard T. Farias

December 2020

Thesis Advisor: Carolyn C. Halladay
Second Reader: Zachary Shore

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE DRONE AMERICA: THE END OF PRIVACY?	**5. FUNDING NUMBERS**
6. AUTHOR(S) Richard T. Farias	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Cutting-edge technological innovations have enabled law enforcement agencies to collect data over a geographical area in relatively short amounts of time. Drones (also known as unmanned aerial vehicles) are becoming increasingly acceptable and employed by state and local law enforcement to become force multipliers. While the Federal Aviation Administration has addressed the integration and safety of flight requirements for law enforcement agencies to utilize drones, federal privacy and data collection regulations are unresolved.

This thesis argues that federal regulation is required and attempts to highlight the distinction between surveillance technology and delivery platforms to understand how to approach the regulation of data gathering.

In doing so, this thesis uses a political, economic, socio-cultural, and technological (PEST) analysis to examine Title III and relative jurisprudence dealing with both surveillance and aerial platforms. The PEST analysis aims to bring forward the salient points in crafting recommendations and expansion in current legislation that support an increase in citizens' safety and security, but remain within the bounds of constitutional liberty and the Fourth Amendment.

14. SUBJECT TERMS drones, privacy, public safety, local law enforcement, policy	**15. NUMBER OF PAGES** 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DRONE AMERICA: THE END OF PRIVACY?

Richard T. Farias
Lieutenant Commander, United States Navy
BGS, Columbia College, 2009

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: Carolyn C. Halladay
Advisor

Zachary Shore
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cutting-edge technological innovations have enabled law enforcement agencies to collect data over a geographical area in relatively short amounts of time. Drones (also known as unmanned aerial vehicles) are becoming increasingly acceptable and employed by state and local law enforcement to become force multipliers. While the Federal Aviation Administration has addressed the integration and safety of flight requirements for law enforcement agencies to utilize drones, federal privacy and data collection regulations are unresolved.

This thesis argues that federal regulation is required and attempts to highlight the distinction between surveillance technology and delivery platforms to understand how to approach the regulation of data gathering.

In doing so, this thesis uses a political, economic, socio-cultural, and technological (PEST) analysis to examine Title III and relative jurisprudence dealing with both surveillance and aerial platforms. The PEST analysis aims to bring forward the salient points in crafting recommendations and expansion in current legislation that support an increase in citizens' safety and security, but remain within the bounds of constitutional liberty and the Fourth Amendment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AFR	automated facial recognition technology
AGL	above ground level
CALEA	Communications Assistance for Law Enforcement Act
CBP	Customs and Border Patrol
CCTV	closed-circuit television
COTS	commercial-off-the-shelf
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DJI	Da-Jang Innovations
DOJ	Department of Justice
ECPA	Electronic Communication Privacy Act
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FBI	Federal Bureau of Investigations
FRT	facial recognition technology
GPS	global positional system
LEO	law enforcement officer
NAS	national air space
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OPM	Office of Personnel Management
PEST	political economic social and technical
PII	personal identifiable information
SWAT	special weapons and tactics
SWP	South Wales Police
UAS	unmanned aerial systems
UAV	unmanned aerial vehicles
VFR	visual flight rules

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to express my genuine appreciation to my advisor, Dr. Carolyn Halladay; second reader, Dr. Zachary Shore; the Naval Postgraduate Graduate School Writing Center; and the faculty for their direction and patience during the preparation and finalization of this thesis. Their steadfast and swift advice was vital and contributed immensely throughout the entire writing process.

Most of all, I like to thank my wife, Kristin. During this whole program, she was my rock and selflessly put up with the long nights, schooling the kids, and providing guidance while working from home. She is the backbone of our family and made this thesis feasible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A nation-state's ability to access, control, and continuously monitor within its borders is paramount to ensuring its citizens' safety and security. Cutting-edge technological innovations have enabled law enforcement agencies to collect intelligence over vast geographical areas in comparatively short amounts of time. However, how much is too much—surveillance, intelligence—or information?

A. RESEARCH QUESTIONS

In light of recent technological advances, how can state and local law enforcement agencies effectively employ drones to increase the safety and security of public spaces within the United States without infringing on the privacy of U.S. citizens?

Should domestic law enforcement agencies expand to provide protection and intelligence collection through the use of drones (also known as unmanned aerial systems or vehicles, UAS or UAV) within U.S. borders?

B. PROBLEM STATEMENT

Drones and sensing technology are useful now and are apt to become more useful (and widely used) because the technology keeps getting better. The term drone is associated with, and used synonymously with, the sensing and surveillance technology drones carry. Drones, however, are simply another aerial vehicle. Airplanes can legally fly over your home, and under Federal Aviation Administration (FAA) guidelines, drones are no different, which is settled law. Fixating on drones in a sideways attempt to regulate surveillance provides strange results.

Drone-based surveillance technology allows law enforcement to gather large volumes of data that can be useful in enforcing laws, rendering assistance, or providing an unbiased recall of contentious situations. The concern is that modern surveillance technology may infringe on privacy rights because its inherent capability to gather data transcends the standards enacted to protect privacy under the Fourth Amendment. The Fourth Amendment uses specific tests to determine whether privacy expectations are

reasonable and that the original intent and extent of privacy protection enacted when the Fourth Amendment was devised does not diminish over time or with technological advancement.

Clearly, regulation will and does help manage this tension for maximum benefit on all sides. To regulate drone use for law enforcement, a distinction needs to be made between drone platforms and drone-borne surveillance technology. On the one hand, drones are simply aerial vehicles, fundamentally no different from other aerial vehicles that operate in the national air space (NAS). The FAA specifically regulates drones regarding all aspects of operation and licensing. On the other hand, the various perception and surveillance technologies carried aboard drones as "sensor suites" allow operators to survey the environment, perhaps from a distance, and gather data over the course of a flight, perhaps for safety or navigation purposes or perhaps for law-enforcement-related surveillance and data collection. Regulations regarding drone surveillance should rightfully focus on the surveillance aspect and be divorced from the UAV platform.

More or less settled U.S. law holds that aerial search is reasonable because the search is conducted from public vantage points that anyone may reasonably see by looking with their eyes. Drones, as aerial platforms, work in these same public places. However, surveillance platforms have advanced through the use of other-than-visual sensors to allow technology to see through such opaque barriers as walls; these sensors can "see" more than the unaided human eye can. As such, they may conflict with the current legal framework for warrantless surveillance, which, as covered later in this thesis, remains pegged to the standard of human vision.

The byproduct of effective collection is data. Advancements in data processing, storage, and dissemination—like sensor technology itself—have markedly increased in recent years. Data can be captured *en masse* in large-scale surveillance events and warehoused for review at a future date. Data review can be sped up or slowed down to analyze information at a depth not possible with live surveillance. Increases in storage capacity and the reduction in the cost of storage media have created a situation wherein the sheer volume of data being collected has outpaced the ability to analyze it. Where before large-scale data collection and storage was throttled by the physical limitation and financial

cost of storing it, now such storage solutions as cloud computing and streaming media, have largely removed collection and storage constraints. Digitization means data is no longer bound by a physical footprint, and as a result, more and more extraneous data is collected and stored. Due to the overcollection and hoarding of excessive data, commonly referred to as "infobesity," analysts can become overwhelmed ("analysis paralysis") by combing through a sea of data. It is a symptom of technology providing the ability to achieve a result without the throttling mechanism or regulation to curtail it. Data frameworks, for example, the U.S. Privacy Act of 1974, require that federal agencies comply with specific standards in their systems of records to maintain the privacy and accuracy of personal information stored in their databases. From that act came the Code of Fair Information practices that outlined general guidelines limiting the collection, disclosure, use, and security of the data federal agencies maintained on individuals.[1] However, personal information privacy protection guidelines in the Privacy Act of 1974 are too general to curtail or adequately manage drone surveillance data effectively for use in law enforcement.

Although surveillance in public spaces is legal, people are uncomfortable with the idea that they may be filmed by anyone at any time, particularly from a small agile aerial platform, without permission and without knowing who is doing the filming or for what the images will subsequently be used. A lack of transparency in law enforcement data collection and retention policies may increase concern in the community over mundane data gathering when no actual basis for the concern exists. Once data has been captured, an equally undefined access, storage, and retention policy might also breed concern that data might be used for purposes other than for which it was collected, and which might ultimately cause harm to the person at some future time.

Jurisprudence has attempted to determine "reasonableness" of privacy expectations in cases of persistent surveillance, but it has not clearly defined what span of observation time constitutes a violation of privacy. If left ambiguous, this lack of specifics may lead to

[1] Defense Privacy and Civil Liberties Office, *Introduction to The Privacy Act* (Arlington, VA: Defense Privacy and Civil Liberties Office, n.d.), 2, accessed November 18, 2020, https://dpcld.defense.gov/Portals/49/Documents/Privacy/2011%20DPCLO_Intro_Privacy_Act.pdf.

issues when looking at extended drone data collection, either per collection event or over the course of multiple aggregated events. Drone-enabled collection inherently improves the ability of law enforcement to collect large amounts of high-definition data. What remains unresolved is what to do—or not to do—with the data once it is collected.

C. ADVANCING TECHNOLOGY AND SENSOR ACCURACY

Advancements in technology mean that the rationale used as a basis for privacy cases, for example, the ready availability of technology for general public use, may be challenged as a constitutional standard. The first section provides the background on the advancements in technology and miniaturization that allowed increasingly sophisticated sensor suites to be placed on small drones. The second section discusses particular issues and shortcomings surrounding the accuracy and reliability of key sensor technologies central to today's drone capabilities; namely facial recognition technology, the implications of subject misidentification for law enforcement missions and legal prosecutions, and how accuracy impacts the public's perception on bias and usability in a law enforcement capacity moving forward.

1. Advancing Technology

The late 20th century saw an epochal shift from an age characterized by industry to one primarily fueled by technology and information. Moore's Law, which predicted technological obsolescence based on the doubling rate of transistors on an integrated circuit board, and Kryder's Law, which used disk drive density (areal density) improvement to predict future increases in storage capacity, both found that growth in the technology industry occurs exponentially.[2] In similar terms, MAJ Michel Busch discusses UAS minimization trends in line with Moore's Law from the first generation UAS design and capabilities, which were "determined, and limited, by the payload size and weight of the sensors available. During that time, the production of high-definition aerial imagery required a platform which today is called NATO class 2 UAS, weighing between 150 and

[2] Niveditha Pookkottuvariam, "Future of Moore's, Kryder's, and Robert's Laws," Medium, January 26, 2019, https://medium.com/@nivedithaartist/future-of-moores-kryder-s-and-robert-s-laws-27c79ef343a8.

600 kg and requiring dedicated launch and recovery elements."[3] Miniaturization, the fundamental enabler behind Moore's law, has significantly changed today's drone systems' payload capacity and its ability to carry increasingly sophisticated sensor suites. The continued trend of increasingly miniaturized components has equipped today's UAVs with extreme sensor precision and navigational accuracy at a fraction of the previous weight and size. High definition resolution, zoom, and low light image capture capability all surpass the ability of naked human perception. Pairing these sensor suites with drones for use by law enforcement creates ambiguity in current regulations in that drones can effectively see through barriers that human eyes cannot.

Meanwhile, the commercial sector's relentless drive to improve and market technology has precipitated a sharp rise in the development of small, inexpensive, and desirable technological gadgets; from fully integrated voice-activated smart devices to controlling fully networked homes to smartphones and personal visual surveillance devices no larger than a deck of cards, but with the capability to capture, track, and record everything in an individual's immediate world. Today's cheap and accessible nature of surveillance technology has placed it in the hands of the masses, including elements of society who seek to use these technological gains in illicit or illegal applications. Tech that was once only available to military units or specialized segments of society is now widely available and commonly employed. In this way, technology acts as a force multiplier, both for good and for malicious gain. More importantly, it undercuts the argument against allowing technology that can see through walls on the basis that it is not available for general public use, which thus calls into question the unconstitutionality of the equipment.

2. Sensor Accuracy

Law enforcement officers (LEOs) cannot be everywhere, but drones equipped with technology act as a force multiplier to enhance safety and security. At the center of the discussion on drone capability lies a deeper consideration for the accuracy of the sensors employed. Drones rely heavily on the use of sensors to offset the fact that they are not

[3] Michel Busch, "Unmanned Aerial Systems Miniaturization," *Joint Air Power Competence Centre* (blog), March 22, 2018, https://www.japcc.org/unmanned-aerial-systems-miniaturization/.

physically manned. However, sensor accuracy and recognition algorithms designed for basic navigation purposes may not be discriminating enough to meet legal prosecution criteria. One such sensor of particular value to drone surveillance, but with a widely variable accuracy level, is facial recognition technology (FRT).

FRT is one of the more politically charged emergent drone technologies deployed by law enforcement. Current facial recognition technology applications in use by law enforcement agencies (local, federal, and national) include public safety cameras, closed-circuit television (CCTV), and satellite imagery to locate criminals. Software variants commonly used by enforcement agencies include detection algorithms, thermal analysis, and feature and texture analysis. Facial recognition benefits are increased significantly by the agility of drones. Numerous commercial-off-the-shelf (COTS) drones currently employ one or more of these techniques.

Applying innovative methods like FRT to apprehend dangerous individuals is vital to U.S. citizens' security and protection. However, with the potential violation of civil liberties and privacy emerging as a hot issue, both lawmakers and law enforcement officials have articulated valid considerations. Law enforcement officials tend to focus on the necessity of implementing facial recognition software to locate, track, and apprehend criminals, while lawmakers tend to defend the privacy rights of American citizens. Both perspectives are critical in striking a balance between the desire for privacy and the need for effectiveness when employing these capabilities in the public arena.

Additionally, the use of FRT in law enforcement is currently in contention. As Ted Rall, an American columnist and author, writes:

> Cops in a video command center tried to tap into Boston's network of public and (mostly) private surveillance cameras to track the suspects in the 2013 marathon bombing. However, the facial-recognition software system failed to pick up the Tsarnaev brothers as they moved across Boston and its suburbs because its algorithms required full-frontal images for comparison.[4]

[4] Ted Rall, "The Pros and Cons of Facial Recognition; Debate Safety and Civil Liberties before it Becomes Ubiquitous," *Wall Street Journal*, May 2019, Proquest.

As Rall points out, this algorithm-constrained application of facial detection not only proved to be fruitless but also collected non-relevant data on the public lives of citizens. The collection of non-relevant data drives many privacy experts and activists to demand more restrictive legislation on this matter to protect Fourth Amendment rights.

Since the technology used on commercially sourced drones comes largely from developments in private sector applications, private sector statistics are more applicable to the question of sensor and algorithm accuracy than a military-grade counterpart is. For this reason, law enforcement's use of small drones draws from private sector discussions on technological development and algorithm accuracy. As an example, the American Civil Liberties Union (ACLU) heavily criticizes the accuracy of facial recognition software, more specifically Rekognition, the software developed by online retailer Amazon. Although Rekognition is developed for the private sector, it is heavily sought-after by law enforcement agencies, and a prime candidate for drone-based law enforcement surveillance missions. In 2018, the ALCU ran a facial recognition accuracy assessment using Rekognition, and according to their study, "the software incorrectly matched 28 members of Congress, identifying them as other people who have been arrested for a crime."[5] While the implication that 28 members of Congress are criminals may be initially humorous, it sparked grave concerns about the validity of Amazon's product and its use by law enforcement agencies. This imperfection highlights the inherent danger in relying solely on an algorithm for accurate identification. Drones enabled with facial recognition offer a world of new opportunity for law enforcement across the spectrum of missions, but the inherent danger of misidentification remains.

Another concern that surfaced from this study and the rapidly evolving use of this technology is the potential bias against citizens with darker skin. According to the ACLU's assessment, "nearly 40 percent of Rekognition's false matches in our test were of people of color."[6] The inaccuracy of modern-day facial recognition software and privacy concerns

[5] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots," *ACLU* (blog), July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[6] Snow.

led some city legislators across America to enact policy changes prohibiting the use of facial recognition software by local law enforcement agencies. “Boston is now the second-largest city in the world to ban facial recognition technology, behind San Francisco. Five other Massachusetts communities have a ban: Somerville, Brookline, Northampton, Springfield and Cambridge.”[7] Much of the controversy that ignited these movements is due to the publicly held belief that recognition software infringes on the civil rights and liberties of American citizens.

However, shortly after the ACLU assessment was published, Amazon debunked the findings based on the parameters used in the analysis. ACLU studies set the confidence threshold to 80 percent, a threshold well below the 99 percent standards used by law enforcement agencies. The confidence threshold, or percentage of accuracy, set can yield a vastly different data output. It is very unlikely that any judge in the United States would deem that the data gathered from a collection event with a confidence threshold set to 80 percent was reasonable or reliable. Dr. Wood went on record with Amazon’s findings illustrating the importance of implementing strict settings to reduce any doubt when identifying individuals.

> The 80% confidence threshold used by the ACLU is far too low to ensure the accurate identification of individuals; we would expect to see false positives at this level of confidence. We recommend 99% for use cases where highly accurate face similarity matches are important (as indicated in our public documentation). To illustrate the impact of confidence threshold on false positives, we ran a test where we created a face collection using a dataset of over 850,000 faces commonly used in academia. We then used public photos of all members of U.S. Congress (the Senate and House) to search against this collection in a similar way to the ACLU blog. When we set the confidence threshold at 99% (as we recommend in our documentation), our misidentification rate dropped to zero despite the fact that we are comparing against a larger corpus of faces (30x larger than the ACLU test).[8]

[7] Ally Jarmanning, “Boston Bans Use of Facial Recognition Technology. It’s the 2nd-Largest City to Do So,” WBUR News, updated June 24, 2020, https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban.

[8] Matt Wood, “Thoughts on Machine Learning Accuracy,” *AWS News* (blog), July 27, 2018, https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/?tag=theverge02-20.

Currently, the United States does not have a legal framework for LEOs to gather evidence using FRT on drones to prosecute persons of interest for potential crimes they may have committed. However, as an example of a successful model at work, the South Wales Police (SWP) recently settled a case, *Bridges v. CCSWP, and SSHD*, in the United Kingdom that addressed the employment of automated FRT (AFR). The Court addressed consent, civil liberties, and privacy rights infringement with the lens of the emergence of technological advances, for example placing technology on small mobile aerial platforms. They also acknowledged that with sufficient software criterion requirements and adequate safeguards in place to protect the data and privacy of biometric data, they were "satisfied both that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that SWP's use to date of AFR Locate has been consistent with the requirements of the Human Rights Act, and the data protection legislation."[9]

D. LITERATURE REVIEW

The Fourth Amendment's expectation of privacy only applies to the government snooping to find evidence to use against a person. A person has no more expectation of privacy vis-à-vis, say, Google, than what someone may find in the company's formidable user's agreement. Furthermore, the private sector owes no more consideration of a person's privacy than what they pay for. The question at hand is whether the government can use a particular piece of evidence that it has pried out of a citizen's hand or house or hand-held device against said citizen in a court of law. This same question applies to drone-based surveillance of the public. Before law enforcement can reasonably begin employing drones for law enforcement missions, unresolved questions surrounding the use of the technology and platform need to be addressed. The first section examines how jurisprudence regarding the reasonable expectation of privacy adapted to shifts in new technology and capability. The law enforcement's position as to the necessity for drone surveillance to ensure safety and security is outlined. In counter, the position regarding concerns over privacy

[9] "High Court Dismisses Claim for Judicial Review in Facial Recognition Technology Case: Bridges and Another v South Wales Police," Society for Computers and Law, September 4, 2019, https://www.scl.org/news/10656-high-court-dismisses-claim-for-judicial-review-in-facial-recognition-technology-case-bridges-and-another-v-south-wales-police.

infringement and Fourth Amendment are presented. The second section examines surveillance through aerial platforms' lenses to establish the constitutionality of using aerial platforms to capture data and establish limitations on airspace ownership and exclusion. The third section explores data capture and use, including examining how the courts perceive the legality of using technology that can "see" through barriers, as drones currently can do. This section also examines jurisprudence surrounding persistent surveillance, and determining when the limit of the reasonableness of privacy expectations that separates surveillance from search is reached.

1. Privacy: Reasonable Expectation

The Fourth Amendment, often characterized as a "constitutional right to privacy," provides the constitutional basis for "people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" without a legitimate warrant.[10] However, if incriminating objects are in plain view, then a warrant is not necessary. Nothing is more public than someone's face. Following this line of reasoning, characterizing the collection of publicly displayed data (i.e., face) as unreasonable, citing Fourth Amendment protection rights, is paradoxical at best—akin to demanding "public privacy."[11] This section examines how jurisprudence regarding the reasonable expectation of privacy adapted to technology advancements and similarly advances to accommodate drone use profiles.

The privacy granted under the Fourth Amendment is not absolute. Nor does this expectation prevail across all locations and circumstances. *Olmstead v. United States* (1927) acts as a baseline on Fourth Amendment precedent involving the emergence of technological advances.[12] Justice Joseph Bradley emphasized, through the Court's decision, that the majority was not concerned with how evidence was collected as long as

---

[10] "Fourth Amendment," Legal Information Institute, accessed February 24, 2020, https://www.law.cornell.edu/wex/fourth_amendment.

[11] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," *Mississippi Law Journal* 72 (2002): 232, doi:http://dx.doi.org/10.2139/ssrn.364600.

[12] Olmstead v. United States, 277 U.S. 438 (1928), https://www.law.cornell.edu/supremecourt/text/277/438.

it did not violate the sanctity of citizens' homes or their Constitutional protections. Moreover, a lawful search and seizure referred "to the examination of one's person, papers, tangible material effects, or home—not their conversations."[13] The penalty for the state violating a citizen's Fourth Amendment privacy was exclusion of the would-be evidence from court; indeed, roughly 35 years later, the Exclusionary Rule expanded the expectation of privacy rights by deterring agents of the government from gathering and using evidence without cause (unreasonable search and seizure).[14] A few years later, amid significant telephone technology changes, *Katz v United States* (1967) reversed the Supreme Court's position in *Olmstead*. In *Katz*, a mobile recording device was planted by federal agents in the vicinity of a public telephone booth to monitor conversations about illegal gambling.[15] The defense for Charles Katz argued that using evidence obtained from mobile recording technology in a public area without penetrating a physical location was an unconstitutional search and seizure because an individual expects a meaningful level of privacy.[16] In the decision, Justice Harlan affirmed that in an

> enclosed telephone booth, a person has a constitutionally protected reasonable expectation of privacy; that electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment, and that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.[17]

Katz clearly expanded an individual's privacy rights beyond the home (*Olmstead*), along with establishing how evidence obtained through technology relates to electronic surveillance. By extending privacy to a public structure not owned by the individual being surveilled, this decision clarified that the public and private line for Fourth Amendment protections is not quite as clear-cut as persons, houses, papers, and effects in practice.

---

13 "Olmstead v. United States," Oyez, accessed December 3, 2020, https://www.oyez.org/cases/1900-1940/277us438.

14 "Exclusionary Rule," Legal Information Institute, accessed November 11, 2020, https://www.law.cornell.edu/wex/exclusionary_rule.

15 Katz v. United States, 389 U.S. 347 (1967), https://www.law.cornell.edu/supremecourt/text/389/347.

16 "Katz v. United States," Oyez, accessed November 11, 2020, https://www.oyez.org/cases/1967/35.

17 *Katz*, 389 U.S. 347.

2. Privacy vs. Security: Two Cases

Polarized opinions concerning privacy rights and civil liberties on one side march in strong counterpoint to law enforcement's ability to capitalize on technology for the nation's safety and security. The following two sections lay out the supporting viewpoint for using drones for law enforcement and opposing viewpoints from those who feel that drone use will infringe on privacy.

a. The Case for Drone Collection, or Law Enforcement's Position

Testimony from Chief Vasque, of the Lawrence Police Department, indicates that drones are a proven force multiplier across the spectrum of law enforcement missions and are critical to ensuring U.S. citizens' safety and security.[18] A 2016 National Institute of Justice report highlighted that numerous examples of the successful employment of drones along the country's border zones support those drones' employment throughout the country's interior poses little risk to privacy when clear limitations are imposed through regulation and appropriate-use guidelines.[19]

Department of Homeland Security (DHS) agencies employ various types, models, and series UAS throughout the country. The Customs and Border Patrol (CBP) Air and Marine Operations department operates a diverse fleet of vehicles ranging from Predator B drones to handheld units, and each has a specific mission based on its payload. The ability to maintain a "God's eye" vantage point with drone-borne sensors allows the DHS and other agencies a distinct advantage that capitalizes on the capacity to collect data through sophisticated technology. Along with precise locations, patrolling agents are relayed time-critical intelligence information updates as situations escalate. These updates give agents a current situational report—a critical advantage in volatile situations—so they know what to expect once they arrive on-scene. Intelligence provided by drones gives the

[18] Jill Harmacinski, "Eyes in the Sky: Drones a 'Force Multiplier' for Lawrence Police Department," *The Eagle Tribune*, October 17, 2020, https://www.eagletribune.com/news/merrimack_valley/eyes-in-the-sky-drones-a-force-multiplier-for-lawrence-police-department/article_f128491f-a33f-5aaf-ac9c-47743aa16ac2.html.

[19] Nancy Rodriguez et al., *Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program*, NCJ 250283 (Washington, DC: National Institute of Justice, 2016), 102, https://www.ncjrs.gov/pdffiles1/nij/250283.pdf.

law enforcement agents involved a sense of domain awareness and allows them to prioritize their courses of action during dynamic or extended pursuits.[20] Although on a smaller scale than the military-spec counterpart, flying COTS drone systems over volatile domestic situations provide state and local law enforcement personnel the same situational awareness, which enhances the team's safety and effectiveness.

UAS have a growing role in another kind of protection, search and rescue. The use of drones during search and rescue operations is a force multiplier in situations where human resources are inadequate, accessibility to the operating area and intelligence is limited, or when a natural disaster occurs. In 2018, experienced first responder UAV operators worked with the DHS to provide feedback on drones' employment in the field. The drone focus group indicated, "small drones offer tremendous potential for emergency response missions. Thanks to recent [technological] advances, they have become more effective, more affordable, and easier to fly. They can not only keep responders safer but also provide opportunities for missions impossible for manned aircraft, such as exploring inside buildings and tunnels."[21]

b. The Case against Drone Collection, or the Privacy Position

While the use of multi-sensor and highly capable drones for intelligence gathering and establishing communications networks are appealing for law enforcement and first responders, privacy concerns have been raised over the sensors UAVs may carry when employed by the U.S. government in citizens' backyards instead of on the soil of a foreign battleground or nation-state. FRT, thermal imagery, and other high-tech, adaptive sensors capture not only targeted information but also secondary data involving individuals not a part of the investigation. The ACLU and other civil rights organizations heavily criticize

[20] "Eagle Pass CBP Officers Seize over $300K of Narcotics at Port," U.S. Customs and Border Protection, January 23, 2017, https://www.cbp.gov/newsroom/local-media-release/eagle-pass-cbp-officers-seize-over-300k-narcotics-port.

[21] "Snapshot: First Responders Assess Drones for Search and Rescue Missions," Department of Homeland Security, April 2, 2020, https://www.dhs.gov/science-and-technology/news/2020/04/02/snapshot-first-responders-assess-drones-search-and-rescue-missions.

facial recognition software and surveillance conducted on American citizens.[22] Specifically, the ACLU maintains a firm stance that the deployment of drones

> without proper regulation, drones equipped with facial recognition software, infrared technology, and speakers capable of monitoring personal conversations would cause unprecedented invasions of our privacy rights. Interconnected drones could enable mass tracking of vehicles and people in wide areas. Tiny drones could go completely unnoticed while peering into the window of a home or place of worship.[23]

Agencies outside of the DHS's realm (Federal Bureau of Investigations (FBI), Drug Enforcement Agency (DEA), other states, and local law enforcement agencies) have contracted for the employment of DHS drones to gather intelligence data. A very recent example is the deployment of an "unmanned [CBP] aircraft to help provide situational awareness for federal law enforcement partners in Minneapolis" during the George Floyd protests.[24] The agency that requested the surveillance support was not identified, and the CBP promptly recalled its UAV to its home base in North Dakota. The ACLU's position is that flying military-grade drones over domestic political protests is an overstep by an agency federally funded to operate surveillance on the border, as authorized by Congress.[25] However, no clear federal legislation restricts the overflight of drones over peaceful protests in a law enforcement capacity. This ambiguity calls into sharp focus the question of how legislators who sit on oversight committees can ensure Fourth Amendment rights are upheld during homeland surveillance. The ACLU's privacy and technology department indicated:

> The public outcry has made it clear that if law enforcement is to benefit from sUAS use, they must involve the community in the process, being

---

[22] Jacob Snow, "Amazon's Disturbing Plan to Add Face Surveillance to Your Front Door," American Civil Liberties Union, December 12, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-your.

[23] "Domestic Drones," American Civil Liberties Union, accessed June 5, 2020, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

[24] Geneva Sands, "Customs and Border Protection Drone Flew over Minneapolis to Provide Live Video to Law Enforcement," CNN, May 29, 2020, https://www.cnn.com/2020/05/29/politics/cbp-drone-minneapolis/index.html.

[25] Jay Stanley, "Protests, Aerial Surveillance, and Police Defunding," American Civil Liberties Union, June 24, 2020, https://www.aclu.org/news/national-security/protests-aerial-surveillance-and-police-defunding/.

> transparent on the benefits and risks and on the safeguards that will be put in place to protect public privacy and safety. Strong community relationships and communication can ensure that sUAS become community assets used to solve community problems.[26]

UAS are currently regulated to ensure safe operation in the NAS but are not governed by similar regulations regarding acceptable use for surveillance. Therefore, before adopting UAS for law enforcement purposes, a consensus on regulation is needed to prevent privacy infringement and data mismanagement.

E. RESEARCH DESIGN

This thesis analyzes two different approaches to solving the problem: (1) regulating technology (collection) prior to a surveillance event by amending the existing federal statute, and (2) regulating data collection and use after it has been collected, regardless of the means used. The findings of the analyses were subsequently evaluated against three criteria to determine success: (1) what constitutes an effective employment of drones, (2) how to measure the safety and security of public spaces, and (3) how to determine subsequent improvement in safety and security associated with the use of drones

Specifically, this thesis entails a policy options analysis that uses the PEST (political, economic, socio-cultural, and technological) analysis framework, a strategic tool originally developed to help businesses succeed by understanding "big picture" impacts in the form of opportunities and threats beyond the control of the business. The PEST analysis framework (Appendix A) examined macro-environmental factors using environmental scanning to identify opportunities and threats in the external environment to understand factors better that affect the organization and generate policy recommendations. The PEST analysis identified gaps, seams, and areas for change necessary to recommend the best policy option for the safe, effective employment of drones while respecting legitimate privacy concerns. The following concerns are underlying core concerns (gaps) recognized

[26] Maria Valdovinos, James Specht, and Jennifer Zeunik, *Community Policing & Unmanned Aircraft Systems (UAS): Guidelines to Enhance Community Trust* (Washington, DC: Office of Community Oriented Policing Services, 2016), 2, https://rems.ed.gov/docs/COPS_Community-Policing-UAS.pdf.

by community experts and privacy advocates to enable a way forward in developing federal and state legislation, as well as policy options.[27]

- Concern 1: No consistent guidelines and limitations exist to control or regulate visual surveillance in the United States.
- Concern 2: No core consensus exists among state regulations that provide guidelines for the employment of visual surveillance in public, nor does a consensus on penalties for violations.
- Concern 3: No policy or legislative framework exist governing data retention, access, archive, and deletion in conjunction with law enforcement UAS surveillance data collection.
- Concern 4: No sufficient jurisprudence exists to steer the operation of UAS clearly for law enforcement purposes in light of new technological capabilities that enhance observation beyond "naked-eye aerial observation."[28]
- Concern 5: A consensual intercept framework needs to be established to authorize law enforcement to continue recording in constitutionally protected arenas in cases of contested authorization, for example, in situations of domestic abuse or when anyone but not all involved parties have authorized surveillance.

Using PEST, data was sorted into four categories, and an analysis was performed to determine the feasibility of implementing each solution from the standpoints of political

[27] "Big Data," American Civil Liberties Union, accessed November 23, 2020, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/big-data; Stanley, "Protests, Aerial Surveillance, and Police Defunding"; Gregory McNeal, "Drones and Aerial Surveillance: Considerations for Legislatures," *Brookings* (blog), November 13, 2014, https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/; National Telecommunications and Information Administration, *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability Consensus, Stakeholder-Drafted Best Practices Created in the NTIA-Convened Multistakeholder Process* (Washington, DC: National Telecommunications and Information Administration, 2016), 3, https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

[28] "California v. Ciraolo," Oyez, accessed March 8, 2020, https://www.oyez.org/cases/1985/84-1513.

practicality, economic viability, the socio-cultural likelihood of acceptance, and technological feasibility. PEST analysis also yielded stakeholder preference for the five key players: public, law enforcement, ACLU, government, and business. The scope of this study accepts five key assumptions when examining the feasibility of the solution:

- Privacy expectations continue to remain at currently reduced levels or have further declined with the mass public acceptance of widely available advanced technological devices.
- No established federal limits are placed on visual surveillance of public spaces, excepting such spaces considered public-private as restrooms and changing areas.
- All spaces with public access will be treated as public space, with no reasonable expectation of privacy during the time the public is reasonably expected to have access to that particular area.
- In any case where it is in the best interest to the safety of law enforcement personnel or other citizens, visual surveillance methods that provide live visual feedback without data capture are authorized for use, to include easements and in transit.
- Visual surveillance enhanced by technological aids (drones, scopes, or sensors) is treated as the legal equivalent of in-person visual observation.

Proposed metrics to demonstrate policy success after implementation include reductions in the number of use-of-force incidents and public complaints against LEOs, reductions in line-of-duty injuries and incident reports for LEOs, increased event recollection accuracy of police reporting using captured data to corroborate narratives and reduce reliance on memory under duress, improved police practices and response methods based on an after-incident review of the footage, a reduction in bias and an increase in the reliability of data used for prosecution as measured by a decrease in data procedurally excluded at trial, and a reduced trial burden as determined by an increase in the number of cases resolved by plea deals using drone-captured evidence.

Analyzing policy options through the lens of PEST provides the most relevant look at "trends and occurrences in an organization's internal and external environment that bear on its success, currently and in the future. The results are extremely useful in shaping goals and strategies."[29] While primary research in the form of surveys may have the potential to yield a more accurate, tailored stakeholder preference response, the sample size required to achieve meaningful results would offset the slight increase in overall data accuracy over other secondary research methods. PEST provides a diverse look at the current attitude toward technology-driven surveillance and yields the most promising angle for developing a knowledge base for predicting acceptance and preference for drone-surveillance regulation in the future. As such, the outcome of the evaluation determined a solution that presents the best balance of regulation and oversight under the constraints of protecting privacy and maximizing technological capability.

F. OVERVIEW OF CHAPTERS

This thesis primarily focuses on technology, surveillance, and public acceptance centralized around the employment of drone-enhanced capability throughout the contiguous United States. Chapter I presents opposing perspectives; the case for and against the use of technology to increase surveillance capability on U.S. soil, and provides in-depth insight into technology's public evolution within the context of the Fourth Amendment. Chapter II discusses modern-day surveillance and Title III through the lens of the Department of Justice (DOJ). Chapters III and IV present two optimized solutions for the regulation of drone-based technology and visual surveillance, and the control of data collected during drone surveillance. Finally, Chapter V presents a discussion and makes recommendations for establishing the best balance of regulation and oversight under the constraints of protecting privacy and maximizing technological capability as a framework for incorporating future innovations.

[29] "Conducting an Environmental Scan," Fordham University, accessed November 4, 2020, https://www.fordham.edu/info/26625/conducting_an_environmental_scan#.

II. LEGAL FRAMEWORK AND GAPS

This chapter covers a history of Title III surveillance, legal frameworks, aerial platforms, data capture, and gaps in the United States. During the discussion of Title III, this section covers what it set out to do, what it achieved, where it failed, and how it needs to adapt to remain relevant as technology continues to advance. This chapter also reviews aerial observation and data capture cases to illustrate tradeoffs of gaining capability and privacy. As it stands, Title III is an excellent baseline to expanding regulation to address finding a middle ground between preserving liberty and providing security. Existing regulation establishes why Title III came about, what it achieved, what it fails to do, and what it needs to address gaps when dealing with drone-borne technology. Consternation exists surrounding the use of technology to "observe" someone beyond the capability of the human physical limitation that stems from a fear of the "unknown." Questions arise in the minds of the people being surveilled as to "what" and "why" someone captured data and "how" they intend to use that data moving forward. When the intent is known, many people willingly subject themselves to video capture and data use, as is the case of on-the-scene interviews, reporting for news stories, or publicizing and promoting programs, for example school district media pages.

A. TITLE III AND SURVEILLANCE

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 is a comprehensive legislative scheme that plays at the heart of this discussion and balances the right to privacy against a bona fide need to gather the intelligence critical to countering criminal activity and enforcing the law.[30] Title III governs most forms of electronic surveillance today, but it does not address either visual surveillance or penetrating surveillance like thermal- or sonar-based technology. Title III is well suited to expanding its framework to capture these and other sensors yet to be developed. Electronic technology

[30] "28. Electronic Surveillance—Title III Applications," Department of Justice Archives, February 19, 2015, https://www.justice.gov/archives/jm/criminal-resource-manual-28-electronic-surveillance-title-iii-applications.

provides an effective but also potentially highly intrusive tool for conducting surveillance. It is so effective, in fact, that regulations banning and then specifically reenabling intercept technology spawned from a series of legal decisions in the 1960s, led by *Katz v. United States* in 1967, when electronic communications of all sorts were becoming ubiquitous in the United States.[31] In 1968, Congress advanced the first specific legal framework for electronic surveillance in the form of Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[32]

Title III prohibits aural, electronic surveillance and interception; it also exempts and strictly regulates specific deviations for law enforcement personnel subject to minimization and other established criteria. While this act served to restore law enforcement's ability to intercept communications information, it quickly suffered from obsolescence itself in the face of technology industry growth. Even something as mundane as determining how to interpret the word "mobile," as used in the mobile interception device referenced in 18 U.S.C 2518(3), can drastically change the interpretation of the legality of law enforcement's actions conducting surveillance. The 7th circuit (*United States v. Ramirez*) interpreted the word "mobile" to mean something that would intercept "mobile" devices—for example cell phones—that by design, were not tied to a specific location.[33] The 5th circuit, in a per curiam decision (*United States v. North*), took a different stance on the interpretation of "mobile intercept device," and chose instead to focus on the mobility of the actual intercepting technology.[34] This interpretation, generally associated with the oral listening device commonly referred to as a "bug," also aligns with the style of collection characterized by the use of UAS.

Title III was further amended in 1994 by the Communications Assistance for Law Enforcement Act (CALEA), which "requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they are

---

[31] Oyez, "Katz v. United States."

[32] "Title III of The Omnibus Crime Control and Safe Streets Act of 1968," Justice Information Sharing, accessed October 20, 2020, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.

[33] United States v. Ramirez, 112 F.3d 849 (7th Cir. 1997), https://casetext.com/case/us-v-ramirez-58.

[34] United States v. North (5th Cir. Aug. 26, 2013), https://casetext.com/case/united-states-v-north-16.

able to comply with authorized electronic surveillance actions."[35] This modification made the wiretapping process easier for agencies to tap digital telephone lines and added language for email and internet service providers to assist in intercepting electronic communications. Title III was also amended by the Patriot Act (2015) to assist law enforcement in terror-related crimes. Both of these updates fall outside the scope of this discussion.[36]

1. What It Set Out To Do

Title III requires:

> Compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted. Many of the restrictions on the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution [and] several of Title III's provisions are more restrictive than what is required by the Fourth Amendment.[37]

Title III set out specific requirements for conducting wiretaps, and using reasonable suspicion and probable cause to establish a foundation to obtain a lawful warrant. It applies specifically to monitoring the content of communications intercepted over wire, and more specifically, telephone conversations.

As amended in 1986 by the Electronic Communications Privacy Act (ECPA), Title III defines three broad categories of communications under the umbrella of permissible surveillance based on their transmission media: spoken, wire, and electronic.[38] Oral (voice) transmission encompasses the intercept of the spoken word during the propagation of sound through open air, as that captured by using a bug or other co-located listening device.

---

[35] Patricia Moloney Figliola, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, CRS Report No. RL30677 (Washington, DC: Congressional Research Service, 2007), CRS-1, https://fas.org/sgp/crs/intel/RL30677.pdf.

[36] History com Editors, "Patriot Act," History, December 19, 2017, https://www.history.com/topics/21st-century/patriot-act.

[37] "9-7.000—Electronic Surveillance," Department of Justice, February 19, 2015, https://www.justice.gov/jm/jm-9-7000-electronic-surveillance.

[38] Title III of The Omnibus Crime Control and Safe Streets Act of 1968.

Wire (voice) surveillance intercepts transmissions traveling through traditional wires, cables, or optical media. The third category, electronic, acts as a catchall for other forms of non-voice communications data transmitted digitally through media that falls outside the scope of oral or wire transmission. Though often classified as a surveillance tool in their own right, drone systems are fundamentally carriers of independent interception technologies. Drones, as a technology, are often the targets of misguided legislation whose actual purpose is to regulate surveillance technology. Drones are aerial platforms, and as such, are already regulated by the FAA. Separating drones and the sensor drones carry is an important distinction to make in the broader discussion of legality and the scope of their employment.

2. What It Achieved

To date, Title III has very adequately addressed privacy concerns for the technology it regulates by incorporating minimization techniques that limit how and when it is legal to infringe on a person's right to privacy in private places. Surveillance technology is intrusive. Title III recognizes that intrusion and functions to prohibit both the interception and disclosure of wire, oral, or electronic communications for all but a few very specific applications sanctioned by the statute, to include highly regulated use by law enforcement agencies.[39] It restricts the use of communications surveillance to valid and vetted requests by law enforcement agencies who first must demonstrate that the request has been made based on probable cause and other criteria set forth by statutes and the constitution. It further establishes significant penalties for misuse, including fines, possible suppression of evidence, and disciplinary action against an investigative officer or LEO.

In deference to Title III, the DOJ has codified electronic surveillance under title nine, chapter seven of the Justice Manual covering the

> specific mechanisms, including applicable approval requirements, for the use of wiretaps, 'bugs' (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral

[39] "18 U.S. Code Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications," Legal Information Institute, accessed August 10, 2020, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

> communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance.[40]

According to the DOJ, "Title III, by its definition of oral communications, permits Federal agents to engage in warrantless interceptions of oral communications when the communicating parties have no justifiable expectation of privacy."[41] In cases where consent is given or met, warrantless interception is allowed in situations that may generally require Title III authorization; specifically telephone, oral, or electronic communications.[42]

Approval for surveillance is required in advance of the collection. The request must be submitted to the DOJ for review before being submitted to a court of competent jurisdiction for authorization. Applications are reviewed in a thorough process to ensure that rigorous standards are applied to each request to confirm that the surveillance is both valid and necessary and that other less intrusive means could not provide a similar result.

> Title III applications uniquely require an additional showing of necessity. The government's application must provide a 'full and complete statement' describing all other investigative techniques that have been tried and failed or explaining why such techniques are likely to be unsuccessful or too dangerous—18 U.S.C. § 2518(1)(c). The court must determine that 'normal investigative procedures' have been or would be unsuccessful or excessively dangerous. Id. § 2518(3)(c).[43]

Title III interception of wire and oral communications is further limited to only the specific crimes listed in 18 U.S.C § 2516(1).

Upon completion of the Title III electronic surveillance, under 18 U.S.C 2518 (8)(a):

> The recording of the contents of any wire, oral, or electronic communication shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order,

---

40 Department of Justice, "9-7.000—Electronic Surveillance."

41 Department of Justice.

42 United States v. Caceres, 440 U.S. 741 (1979), https://supreme.justia.com/cases/federal/us/440/741/.

43 Timothy Crudo and Nicholas Lin, *Wiretapping for Beginners* (New York: Law360, 2011), 3, https://m.lw.com/thoughtLeadership/wiretapping-basics.

> or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions.[44]

Once sealed, the applications and contents are protected from tampering or alteration, and the privacy of persons not charged can be ensured using a Rule 16 protective order applied to "forbid public disclosure of the contents of the materials" coincidentally captured in the course of the authorized surveillance.[45]

3. Where It Failed

By 1986, to remain relevant to the technological conversation and continue to provide a reasonable compromise between the rights of individuals and law enforcement needs, Congress passed the Electronic Communications Privacy Act.[46] Then, as now, it became eminently clear that the existing framework no longer adequately captured the technology capabilities of the day. As became evident in the time before Title III, the loss of surveillance capability by law enforcement is detrimental to mission success.

When Title III was amended in 1986, the resulting legislation defined three broad categories of communications that could be intercepted.[47] Those categories fundamentally translate into voice and data. According to the ACLU, visual surveillance, arguably one of the most invasive forms of collecting data on a target is one of the least-consistently regulated of the collection tools.[48] Laws differ significantly from state to state, but generally, all adhere to the general provision of a "right to reasonable expectation of privacy" under the Fourth Amendment. Regulation varies greatly, from designating specific areas off-limits to surveillance, for example, bathrooms or changing rooms, to a requirement to notify customers and employees of the existence of cameras on a property,

---

[44] "18 U.S. Code § 2518—Procedure for Interception of Wire, Oral, or Electronic Communications," Legal Information Institute, accessed August 10, 2020, https://www.law.cornell.edu/uscode/text/18/2518.

[45] Department of Justice, "9-7.000—Electronic Surveillance."

[46] Electronic Communications Privacy Act of 1986, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

[47] Title III of The Omnibus Crime Control and Safe Streets Act of 1968.

[48] "What's Wrong with Public Video Surveillance?," American Civil Liberties Union, March 2002, https://www.aclu.org/other/whats-wrong-public-video-surveillance.

to rights to privacy being wholly forfeited and void upon a posted notice advising the public that a video camera is in use.[49] In cases where there is a reasonable expectation of privacy, pursuant to DOJ order 985–82, the authority to review requests for law enforcement CCTV video surveillance purposes rests with specific officials of the DOJ Criminal Division under rule 41 of the Federal Rules of Criminal Procedure and the All Writs Act.[50]

Since video surveillance laws vary significantly from state to state, they offer almost arbitrary limitations on how and when an entity may conduct surveillance on the public at large. Unlike its counterparts in voice and data capture, video surveillance is not prohibited by 18 U.S.C. § 2511.[51] Fundamentally, just about anyone with a camera can point it into the public realm right now and capture just whatever they please without consequence. This "open-season" video capture mentality is especially true of service-centric businesses and such venues as libraries, casinos, restaurants, theme parks, and public sports or recreation facilities. Patronage of these venues implies consent to be monitored while on or near the premises, whether the party being surveilled has actually consented or not.[52] While the majority of data collected is likely never going to be used for the purpose it was initially collected, nothing is preventing its use or disclosure in any way, and for any means, the collector deems fit after the fact. The ubiquitous nature of video capture in society today suggests that a hard look at visual surveillance, and all its various aspects, is perhaps overdue.

No clear, standing consensus has been reached when it comes to regulating video surveillance. Video surveillance is already established and pervasive throughout society. Video capture technology has been used by citizens to protect their homes (Ring Flying

---

49 "Video Surveillance Laws by State: Everything You Need to Know," UpCounsel, accessed August 10, 2020, https://www.upcounsel.com/video-surveillance-laws-by-state.

50 "32. Video Surveillance—Use of Closed-Circuit Television (CCTV)," Department of Justice Archives, February 19, 2015, https://www.justice.gov/archives/jm/criminal-resource-manual-32-video-surveillance-use-closed-circuit-television-cctv.

51 "18 U.S. Code § 2511—Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited," Legal Information Institute, accessed October 20, 2020, https://www.law.cornell.edu/uscode/text/18/2511.

52 Jackie Valley, "You're Being Watched: Inside Las Vegas' Surveillance Culture," *Las Vegas Sun*, October 5, 2014, https://lasvegassun.com/youre-being-watched/.

Security Drone), de-escalate arguments (social media live feed), and monitor activities (Nest) for years. Smartphones are used to record video clips of everything from personal celebrations at restaurants to sporting events and beyond, often collaterally capturing countless unwitting spectators and employees in the process. It would be untenable to attempt to regulate or criminalize every inadvertent capture of third-party activity in the public arena. Furthermore, U.S. society is living in a time that has seen a generational shift in privacy mindset from "big brother" and "cold war secrecy" to "#Me Too." The rising generation lives out of the shadows and has spurned movements of openness that have prompted all generations to expose data and behaviors historically made possible by an outdated "culture of shame" mentality. Society has similarly shifted its definition of privacy to accommodate video capture technology as an acceptable "norm."[53] In accepting public video surveillance as a "norm" for private citizens, society must also accept an equivalent level of access when agents in the enforcement of laws employ that technology.

4. What Remains to be Fixed

This discussion stipulates that the existing framework and constitutional rights under Title III are adequate for protecting privacy and sufficiently limited in scope to hold up under scrutiny under the Fourth Amendment's constitutional framework for the surveillance methods it covers. However, to continue to be relevant to today's conversation, Title III is due for an expansion. When Title III was originally conceived in 1968, no one could have envisioned a future wherein technology could have advanced to the degree it has today. Now in the form of smartphones and networked information systems, the average person has access to tools with the ability to provide the combined accumulated knowledge of the human race at the touch of a button on a device the size of a human hand. These same tools and capabilities should not be withheld from law enforcement.

[53] Janna Anderson and Lee Rainie, "Stories from Experts about the Impact of Digital Life, 3. Fifty-fifty Anecdotes: How Digital Life Has Been both Positive and Negative," *Pew Research Center: Internet, Science & Tech* (blog), July 3, 2018, https://www.pewresearch.org/internet/2018/07/03/fifty-fifty-anecdotes-how-digital-life-has-been-both-positive-and-negative/.

Without a clear framework, federal or otherwise, on visual surveillance in the public sector, it is difficult for law enforcement agencies to employ drones effectively in society to enhance safety and security, both for the public at large and for the officers themselves. Senators and Congressmen have attempted to establish privacy regulations, limitations, and transparency but have had little success.[54] Much of this discussion plays out in the public arena at large, where inherent privacy or any right to such does not exist.

B. AERIAL SURVEILLANCE PLATFORMS VERSUS SENSORS

The implementation of technology to conduct observation (surveillance) is overt. Most COTS drones are visible to the eye and audible on the ground at the ranges at which they are flown to observe and collect on targets. This observation is equivalent to equipping a uniformed officer with a body-mounted camera.[55] High-altitude drone systems like those employed by the military and the DHS are out of sight and mind but still not technically covert observation tools. High altitude employment of UAS is less likely to be noticed by the public at large, and the cost of employment precludes this type of tool from becoming an everyday daily use system. Geopositioned surveillance falls outside the scope of this discussion.

Under the ECPA amendment to Title III, roving interception is the authorization to surveil a specific person of interest without specifying a location where the interception will take place. It is generally sought and granted in cases when it is believed that the subject would take actions to thwart collection attempts specifically, and therefore, not practical to do so.

> In essence, the roving intercept provision provides that if federal investigators can show that specification of the particular place for interception of an oral communication is not practical, they may obtain an oral intercept order authorizing them to intercept all of their suspect's face-

[54] Drone Aircraft Privacy and Transparency Act of 2017 (2017-S. 631), https://www.govtrack.us/congress/bills/115/s631.

[55] Matthew Guariglia, "How to Identify Visible (and Invisible) Surveillance at Protests," Electronic Frontier Foundation, June 4, 2020, https://www.eff.org/deeplinks/2020/06/how-identify-visible-and-invisible-surveillance-protests.

> to-face conversations relating to the crime under investigation, no matter where those conversations happen to occur.[56]

The tradeoff in a roving intercept over a standard intercept is that to authorize the surveillance of a person of interest in a non-specific location, the subject must be specifically identified beforehand, rather than listed as "if known." Drones are well suited to perform persistent roving surveillance, and the enabling technology will only continue to improve into the future.

1. Aerial Observation and Public Vantage Point

Among the critical issues with operating drones for surveillance is establishing the airspace from which drones can legally surveil the environment. Looking at drone surveillance through the lens of manned aerial surveillance is the most relevant path to establish the constitutionality of using unmanned aerial platforms to capture data and establish limitations on airspace ownership and exclusion easement and overflight.

United States v. Causby (1946) served to establish an easement altitude over private property of 83 feet.[57] Causby was a chicken farmer, and the low altitude overflight of his property by military aircraft during takeoff and landing from an adjacent field caused his chickens to commit suicide against the barn walls. Seeking compensation under the Fifth Amendment for the loss of his chickens, the minimum altitude of the lowest approach (83 feet above ground level (AGL)), the *Causby* case became the standard for defining the column of airspace associated with the rights of a landowner.[58] Causby's findings held that "airspace, apart from the immediate reaches above the land, is part of the public domain. We need not determine at this time what those precise limits are. Flights over private land are not a taking, unless they are so low and so frequent as to be a direct and immediate

---

[56] Clifford S. Fishman, "Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice," *Georgia Law Review* 22, no. 1 (1987): 49, https://scholarship.law.edu/cgi/viewcontent.cgi?article=1506&context=scholar.

[57] "FindLaw's United States Supreme Court Case and Opinions," Findlaw, accessed November 4, 2020, https://caselaw.findlaw.com/us-supreme-court/328/256.html.

[58] "United States v. Causby," Oyez, accessed November 11, 2020, https://www.oyez.org/cases/1940-1955/328us256.

interference with the enjoyment and use of the land."[59] Since drones are regulated to fly in the NAS, they are required to comply with traffic separation and operating altitudes. For drones under 55 pounds, the maximum allowable altitude is 400 feet above the ground with a maximum speed of 100 mph.[60] No minimum speed is currently associated with small UAS. In practice, UAS pilots would be allowed to transit over private property at will en route to a destination. Piloted aircraft operate in visual flight rules (VFR) using a collision avoidance technique known as see and avoid, without specific legislation in the future directing it. Without a viable technological collision avoidance system in place, drones would also be operating with visual sensors on at all times. Since the most common route of transit for aircraft is direct-line to the destination, the likelihood of routine low-altitude overflight of private property in the normal course of operation is very high.

Flyover surveillance is hardly controversial these days. In the late 1980s, the Santa Clara Police Department received an anonymous drug tip and investigated it. Unfortunately, the police could not "observe the contents of the respondent's yard from ground level because of a 6-foot outer fence and a 10-foot inner fence completely enclosing the yard."[61] The police department then used a private aircraft to fly over the suspected drug dealer's home to observe his backyard. Using photographs obtained through aerial surveillance, the investigating officers collected the data required to obtain a warrant, make the arrest, and convict the perpetrator. The use of the aircraft was necessary to provide the officers with a vantage point they could not achieve from the street level. The offender's motions to dismiss the evidence on the grounds of privacy and alleged Fourth Amendment violations were rejected due to the argument that "any member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[62] While the California Court of Appeals ruled that the search was unreasonable:

> Chief Justice Burger reasoned that the Fourth Amendment protections regarding the home had never been absolute: for example, police officers

[59] Findlaw, "FindLaw's United States Supreme Court Case and Opinions."

[60] FindLaw.

[61] California v. Ciraolo, 476 U.S. 207 (1986), https://www.law.cornell.edu/supremecourt/text/476/207.

[62] *California*, 476 U.S. 207.

> are not obligated to shield their eyes when passing homes on public streets or sidewalks. Since the observations of the Santa Clara officers was nonintrusive and took place within public navigable airspace, their actions were consistent with the Fourth Amendment.[63]

Ciraolo may have built the enclosures to keep his activities private, but his yard was not actually protected from all observation. Findings from *California v. Ciraolo* established that surveillance and observation conducted from a public vantage point that rendered activities clearly visible did not constitute a Fourth Amendment violation.

In the same year as *California v. Ciraolo*, Dow Chemical Company argued that the use of aerial photography by the U.S. Environmental Protection Agency (EPA) over the Dow's Michigan facility on its 2000-acre property constituted a warrantless search, which violated the company's Fourth Amendment rights. According to the 5–4 decision in *Dow Chemical Company v. United States*, "the fact that EPA could take aerial photographs of the facilities from public airspace with the standard photographic equipment employed by mapmakers confirmed that the area was not subject to strict protection from observation."[64] The Court's decision also highlighted that the employment of common-use technologies of the time were an acceptable means to gather evidence as long as they were reasonably accessible to the public.

The *Dow* case, along with that of *Ciraolo*, laid the foundation for *Florida v. Riley* (1989), another case about officers who were able to discern the illegal cultivating of marijuana plants from an airborne vehicle; in this case, a rotorcraft. In Riley's case, officers spotted the marijuana plants through openings in the roof and unenclosed sides of a greenhouse from the air in a helicopter flying 400 feet above ground level. Justice White used the findings from *California v. Ciraolo* to conclude "that a naked-eye police inspection of the backyard of a house from a fixed-wing aircraft at 1,000 feet" did not constitute a search under the Fourth Amendment, and the conclusion that the "respondent could not reasonably have expected that the contents of his greenhouse were protected from

63 Oyez, "California v. Ciraolo."

64 "Dow Chemical Company v. United States," Oyez, accessed March 8, 2020, https://www.oyez.org/cases/1985/84-1259.

public or official inspection from the air, since he left the greenhouse's sides and roof partially open" the court found that he did not have an expectation of privacy.[65] Of note, Justice O'Connor concluded that the FAA safe operational altitude for a specific type of aircraft alone was not the deciding factor for Fourth Amendment constitutionality.[66] Instead, "consistent with Katz, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not 'one that society is prepared to recognize as reasonable."[67]

2. Data: Capture and Use

Thermal imaging devices and other sensors that enhance visual observation beyond the capability of the human limitation are ubiquitous on drones. Further, drones are continuous collectors of data—from using GPS positioning to navigate to visual sensors to see and maneuver around terrain within the environment—a wealth of data is captured. Secondary use of data—data used for other than its original purpose—becomes contentious when it appears that it is being collected under pretext.

In the case of *Kyllo v. United States*, emergent technology with thermal imaging capability was creatively employed by LEOs to determine if Danny Kyllo was growing illegal controlled substances in his home. The thermal imager could not distinguish the identity of objects through the walls of the home, nor could it detect physical movement. The use of this device compared the heat emanating from the home to the heat signatures of surrounding homes. The employment of this sensory-enhancing technology was found to be "not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment search, and is presumptively unreasonable without a warrant."[68] Also, while the argument indicated that there was not a reasonable expectation of privacy, because the thermal device

---

[65] Florida v. Riley, 488 U.S. 445 (1989), https://supreme.justia.com/cases/federal/us/488/445/.

[66] *Florida*, 488 U.S. 445.

[67] *Florida*, 488 U.S. 445.

[68] Kyllo v. United States (Syllabus), 533 U.S. 27 (U.S. Supreme Court 2001).

did not illustrate intimate details, that "all details are intimate details."[69] This case highlights two areas of contention: as technology advances, it will undoubtedly surpass the limits of naked human ability and make its inherent operation able to know things "unknowable without physical intrusion" and a reliable mechanism or standard does not exist to determine what constitutes "general public use." Today, many tools are not in general use because their utility is specific to specialized tradecraft. For example, full-body scanners are commonly employed for airport security but would not necessarily have a broad public use application across other disciplines. In the case of drone-integrated sensors, much like airport body scanners, the functionality would not have a vector for general public use, but would be employed to enhance law enforcement safety and security.

In the case of *United States v. Jones*, the Supreme Court held that Fourth Amendment requirements on searches and seizures bar law enforcement from placing a global positional system (GPS) system on a vehicle to keep track of its location without a warrant.[70] In 2004, officers investigating Jones for suspected drug trafficking employed various investigative techniques, including visual surveillance, to obtain a warrant to place an electronic tracking device on his wife's vehicle. However, the device was installed after the expiration of the time period authorized in the warrant and outside the jurisdiction in which it was issued. Surveillance persisted for a period of 28 days and captured more than 2,000 pages of data. The government obtained a conviction, but Jones moved to suppress the evidence based on a violation of privacy under the Fourth Amendment against unlawful search. This finding was distinguished from the earlier findings in *United States v Knotts* (1983), which held that there was no reasonable expectation of privacy on public roads because the car's movements were knowingly exposed to the public and could have been observed with the naked eye.[71] Although both cases involved the placement of GPS tracking devices to obtain data, the former captured data over an extended period of time, which allowed officers to build a case that could not have been ascertained from a single

[69] Kyllo v. United States, 533 U.S.

[70] United States v. Jones, 565 U.S. 400 (2012), https://supreme.justia.com/cases/federal/us/565/400/.

[71] United States v. Knotts, 460 U.S. 276 (1983), https://supreme.justia.com/cases/federal/us/460/276/.

trip, as in the surveillance of Knotts.[72] In his concurring opinion in *Jones*, Justice Alito outlined issues with the Fourth Amendment and the manner in which they relate to 21st-century surveillance techniques. While he agreed with the judgment, he felt the focus should have instead been on potential privacy violations based on long-term monitoring.[73] This focus is of particular relevance to the discussion on persistent surveillance by drones. Although the type of drones consistent with current-day law enforcement drone use is limited in-flight duration, future miniaturization and technology advancement will continue to extend flight times. The Court's reasoning in *Jones* and similar cases involved a technical trespass (Alito's concurrence) in conjunction with surveillance, but with drones, the surveillance technology itself precludes the need to conduct a physical trespass.[74] Many of the sensors on drones can literally see through walls. Among concerns, Justice Alito expressed in *Jones* included that "coverage of the Fourth Amendment may vary from State to State" based on the state's views on marital and community property, and may serve to create an inconstant standard.[75] Alito also outlined concerns with using the Katz expectation-of-privacy test in cases involving technology. Specifically, Alito discusses that "the Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations."[76] Since one of the two fundamental elements of the Katz tests relies on that stable definition of privacy to determine reasonableness, shifting privacy definitions throws any determination made using Katz's test into doubt. Alito posits that the desire for "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[77] Alito suggests that the best course of action is in line with action taken

[72] "United States v. Jones," Electronic Privacy Information Center, accessed November 11, 2020, https://epic.org/amicus/jones/.

[73] *Jones*, 565 U.S. 400 (2012).

[74] *Jones*, 565 U.S. 400 (2012).

[75] *Jones*, 565 U.S. 400 (2012).

[76] *Jones*, 565 U.S. 400 (2012) at 4A.

[77] *Jones*, 565 U.S. 400 (2012) at 4A.

following *Katz*, which saw Congress take action to resolve the issue by developing a comprehensive statute, rather than leaving the issue to be resolved through court action to develop case law. Justice Alito closes with the acknowledgment that as of 2012, "Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[78] Applying the same process to persistent drone surveillance, a standard for the degree of intrusion a reasonable person may perceive based on a lengthy overflight of public events is unknown.

Emerging technologies continue to push the envelope on surveillance and provide both more sensitive data and an extension of the boundaries delimiting how data is gathered. The capture, use, and re-use of media-data are not well regulated either in public or by government agencies in the United States. Increasingly capable airborne sensor suites continue to influence actions at the forefront of how LEOs conduct investigations, manage public safety, and enhance awareness. During the last century, numerous instances have occurred wherein higher courts have had to intervene to determine whether LEOs' use of technology at that time constituted an unreasonable search and seizure, was protected under the Fourth Amendment, or infringed on other constitutional rights. Drone-based surveillance marks a significant enough advancement in capability to warrant just such a constitutional discussion.

These cases lay the legal bedrock for addressing the regulation and employment of technology as it emerges in the marketplace. Technological advancement is a rapid, dynamic process that will always outpace the ability to legislate and regulate it. Considerations need to be identified as to who has oversight and how the secondary data collected will be ethically utilized. Like most tools, this technology and its byproducts will require maintenance, care, and training for those who operate it. The ability to maintain some semblance of the privacy rights historically enjoyed in the United States will require

78 *Jones*, 565 U.S. 400 (2012) at 5.

a candid look at society's interaction in the current technological landscape and this generation's comfort level at drawing the line between the tradeoffs of gaining capability versus maintaining privacy.

THIS PAGE INTENTIONALLY LEFT BLANK

III. REGULATING TECHNOLOGY PRE-COLLECTION

This chapter examines drone-borne surveillance technology regulation prior to collection events by law enforcement under an expansion of existing Title III regulation to include visual and other technology-enhanced sensors. This policy establishes three distinct areas in which surveillance collection limitations are imposed in conjunction with law enforcement efforts. Private cases align with current requirements for search and seizure as defined constitutionally under the Fourth Amendment. Public cases impose restrictions over identified areas of possible privacy infringement or abuse of power or scope, and business cases recommend regulations and access for law enforcement to surveillance systems run in publicly operated businesses. Effectively regulating and limiting surveillance technology through Title III expansion establishes a pathway for law enforcement to employ surveillance technology, including on drones. PEST analysis identifies major threats and opportunities in the external environment to employing drones in all aspects of the law enforcement mission effectively and provides relevant data to demonstrate the feasibility of implementing this policy.

A. PRE-COLLECTION POLICY

Given the incredibly powerful tools that exist in the market today and into the future, the best solution to exploiting drone-based surveillance and other future technology is to regulate the use of surveillance technology prior to collection events. Drones are a collection platform. They have no more inherent ability to violate privacy than other similar airborne or height-mounted platforms, for example manned aircraft or perches, as supported in jurisprudence regarding the constitutionality of aerial surveillance. To remain relevant with the technological landscape, legislators should look to expand Title III and related legislative schema to encompass all surveillance technology and set guidelines based around defining three cases under which LEOs could surveil and collect data: private, public, and business.

1. Private

In this case, the existing Title III code would be extended to capture visual and other yet-to-be-developed technological forms of surveillance that extend capability beyond natural human limitation. Along with this extension, surveillance authorization and capture of data would be granted in advance of surveillance events under very specific criteria as is required for granting warrants to conduct wiretaps and other directed-surveillance in venues covered under Fourth Amendment privacy laws. Such provisions would include, at a minimum: (1) specific pre-authorization to conduct the surveillance, (2) strict minimization, (3) strict content identification authorizing capture and retention of only pre-identified subject matter, (4) strict identification of aggrieved targets, and (5) federal authorization to conduct the surveillance. Under this extension, law enforcement agents would use the existing legal framework for lawful search and seizure and other applicable regulations to obtain a warrant in advance of surveillance. Once granted, this warrant would authorize roving interception (i.e., drone tracking) and capture of target intelligence, following the aggrieved anywhere, public or private. Methods of surveillance and specific technology would be specified in the warrant in advance of the surveillance event.

2. Public

In this venue, no stricter requirements will be placed on LEOs or agents than is enacted on the average citizen or business operating in general public spaces. Drones and all drone-borne forms of visual surveillance may be employed to enhance the safety and security of public spaces and the safety of the officers and civilians operating in them. This regulation includes a standing authorization to operate drones and use visual surveillance methods over all major public events, planned or unplanned demonstrations, general public crowds and gatherings, and in response to emergent situations developing in public or publicly accessible spaces. Surveillance data collected incidentally in public and commercial spaces not intentionally tied to a specific target (aggrieved) or agenda (criminal action) may still be used to support the request for a Title III warrant application, in line with Fourth Amendment jurisprudence found in *Ciraolo* and related cases. Countering the

argument expressing concern against the use of surveillance data for secondary law enforcement purposes, Gregory McNeal stated "for more than two decades, the police have not been required to turn a blind eye to evidence of criminality merely because they observed it from the air, they similarly should not be required to ignore evidence of criminality merely because they witness the crime through the eyes of a drone."[79] Finally, interference with law enforcement surveillance or surveillance equipment of general public events would be criminalized, which would result in possible fines or imprisonment, or both, for the perpetrator based on the severity of the event.

3. Business

Under this case, businesses with physical public access as part of their operations would be required to apply for a license to operate video surveillance systems inside publicly accessible spaces, regardless of the platform used to employ surveillance sensors. Licenses would be granted by the state through which the business was licensed to operate, requiring periodic training on surveillance regulations, and require the business to subject to inspections for compliance with state and local regulations. Surveillance data use and retention limits would be imposed, and penalties and fines levied against the businesses for violations and infractions. Businesses would further be required to cooperate with valid law enforcement requests for data, in line with 18 USC 2511 (2)(a)(ii).

B. PEST ANALYSIS—MAJOR OPPORTUNITIES AND THREATS

This section covers the major opportunities and threats to regulating surveillance technology from the perspective of political practicality, economic viability, socio-cultural acceptance, and technological feasibility to identify stakeholder preference and examine the feasibility of the proposed policy. This section identifies the benefits of expanding existing regulation, public appeal, and fiscal spending while highlighting drawbacks and fears.

[79] McNeal, "Drones and Aerial Surveillance."

1. Political Practicality

From a political perspective, existing federal regulations governing other technology-based surveillance methods provide a strong framework for expanding drone-based surveillance. Existing regulations very adequately address Fourth Amendment rights and procedures and are backed by years of reasoned jurisprudence. Expanding the umbrella to encompass future technology is the logical next step to ensuring privacy protection in the rollout of new technology.

On the downside, this solution fails to meet the more significant issue of expanding regulations at the speed of innovation. Constantly evolving technology will necessitate numerous future reviews and expansions of this regulation to encompass not-yet-conceived future concepts and creative aggregation and application of existing technologies or it will fall to a conflicting body of case law and regulations, as was the case in *Jones*, which applied 18th-century tort law to reach a decision.[80]

2. Economic Viability

This solution allows law enforcement agencies to obtain the right technology solution for the situation, unit operating capability, and budget from an economic perspective. Small UAS, like those governed under Federal Aviation Regulations (FAR) Part 107, provide a very adequate and easily obtainable technology platform with a fairly easy learning curve.[81] Technology quality is an inherent tradeoff with price point. Low cost commercially available systems, though less capable, are arguably far cheaper to obtain, own, and operate than manned equivalents. According to Capt. Albanese of the Pittsburg Police Department, the $50,000 drone program is but a mere fraction of their $3 million helicopter, without including fuel, maintenance, and inspections.[82]

---

[80] *Jones*, 565 U.S. 400 (2012).

[81] "Fact Sheet—Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)," Federal Aviation Administration, October 6, 2020, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615.

[82] Judith Prieve, "Bay Area Police Agencies Say Drones Are a 'Force Multiplier,'" July 22, 2019, https://www.govtech.com/public-safety/Bay-Area-Police-Agencies-Say-Drones-Are-a-Force-Multiplier.html.

On the downside, similar to other aerial platforms, successful UAS implementation requires long-term funding.[83] Ongoing costs are associated with technology repairs and upgrades, equipment loss, maintenance training and proficiency for operators, and register and license equipment to operate in the NAS. Sources of funding for departments are as of yet unidentified and may require local or federal tax increases and subsidization or the requirement to make other budget tradeoffs to accommodate the operation of drones by law enforcement departments.

3. Socio-Cultural Likelihood of Acceptance

From a socio-cultural perspective, drone use has broad public appeal due to the sheer number of diverse applications enabled by the platform. Drones offer a way for people to photograph or record life events from a new perspective (weddings and sports events), aid in jobs (realtor virtual house walkthroughs), and deliver goods to recipients with speed and ease (medicine, mail, and food delivery). With the right amount of public transparency and limitations on secondary data use, the public has shown to be very receptive to a myriad of drone uses. The likelihood of acceptance for this policy is high because it limits surveillance at the outset of drone engagements and collects only with sensors approved in advance by a warrant granted after demonstrating cause. In the public sector, drone use by law enforcement follows the same rules as everyone else.

On the downside, drone use by law enforcement collects data in the course of operations intended to enforce laws and prosecute violations. Collecting data via drones in the course of law enforcement missions may be seen as more intrusive and suspicious than a physical presence. It is difficult to discern the target of a drone based on its orientation. Further, drone transit (point-to-point) may be perceived as a nuisance. The addition of business sector requirements for surveillance registration and training may be seen as a nuisance. Additionally, granting law enforcement access to data collected by companies in

[83] McNeal, "Drones and Aerial Surveillance."

the course of business will likely be opposed, similar to the FBI attempts at gaining access to Apple technology.[84]

4. Technological Feasibility

From a technological perspective, the hardware, sensors, and algorithms with an immediate benefit to the law enforcement mission set already exist as packages on commercially available UAS in the commercial market. Since 2016, equipped drone suites boast a technology called "Follow-me," programmed to follow a person automatically to capture video.[85] Recognition-based software coupled with vision sensors, namely Da-Jang Innovations (DJI) Activetrack, evaluates pictures live and follows objects or persons marked on the smartphone or the screen on its own.[86] As both tracking and facial recognition accuracy evolves, law enforcement could capitalize on that technology suite to design campus security programs, which would recognize and track students across campus at night. This technology option offers a low-cost way to provide a GPS-enabled live security feed for students throughout campus to enhance security, or in the event of an incident, sound an alert and document the event on video to assist in identifying perpetrators. As facial recognition accuracy improves, drones overhead at such major events as the Boston Marathon can possibly be programmed with the images of known or suspected offenders to aid in prevention and apprehension. Facial recognition also has a role in protecting privacy. By aggregating facial recognition with visual sensors and automatic redaction algorithms, capture events of suspects could blur out non-target faces at the time of data capture to protect against inadvertent third-party privacy intrusion. Facial recognition and GPS tracking are limited prior to collection under the consensual intercept provision when used in public. These technologies are a boon to law enforcement and are authorized directly by the subject being surveilled.

---

84 "The FBI Wanted a Backdoor to the IPhone. Tim Cook Said No," Wired, accessed November 11, 2020, https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

85 Fintan Corrigan, "12 Best Follow Me Drones and Follow You Technology Reviewed," DroneZon, October 18, 2020, https://www.dronezon.com/drone-reviews/best-follow-me-gps-mode-drone-technology-reviewed/.

86 "DJI ActiveTrack Mode Explained," Tom's Tech Time, accessed November 4, 2020, https://www.tomstechtime.com/active-track-mode.

On the downside, limited application occurs under Title III for prosecutions. Drones are an overt surveillance platform, and identifying a drone would allow perpetrators specifically to thwart surveillance efforts or alter criminal behavior. Drones are also vulnerable to spoofing, physical deterrence, and other methods of interference that would render the captured data useless. Timeliness is also a factor. The time required to meet the criteria to gain authorization to surveil a suspect legally may exceed the window of opportunity to gain a relevant visual collection. Planning preceding events is more likely to occur and be captured through data and audio surveillance methods, whereas visual surveillance is more likely to document criminal events in action.

C. ADDRESSING CORE CONCERNS

This proposal adequately addresses core concerns 1 and 2 by providing specific and overarching criteria by which to conduct visual surveillance for law enforcement purposes under an expansion of Title III. Title III has met the requirements of Fourth Amendment constitutionality, and by extension, will provide a mechanism to ensure visual surveillance meets the same. States can craft more restrictive individual policies than Title III, but none may fail to meet the federal minimum surveillance standard.

This proposal adequately addresses core concern 3 by providing a standing federal framework under which all states will be held to the same standards of probable cause, and reasonable suspicion, before the collection of surveillance data is authorized. By extension, visual surveillance data collected will be held to the same rigorous standards already applied to data collected by other surveillance means.

This proposal does not directly address core concern 4, jurisprudence surrounding extending interpretations to beyond natural human observation capability as a standard. However, existing jurisprudence surrounding aerial surveillance from manned platforms and definitions of airspace over private property (curtilage) provide a basis on which to make future determination on the extent to which advances in technology will replace the "naked eye aerial observation" standard observe in *Ciraolo*.[87]

[87] Oyez, "California v. Ciraolo."

Concern 5 falls outside the scope of Title III, and therefore, is not met. As outlined in concern 5, consent issues would instead fall to existing state regulations outside the scope of this proposal.

D. TRADEOFFS AND FEASIBILITY

Under a PEST analysis, the macro-environmental factors examined in an environmental scan inform strategic planning processes. In the following section, the pros and cons of implementing a policy to regulate surveillance technology before collection specific to Title III are examined.

1. Pros and Cons

Updating Title III codifies the appropriate use of visual surveillance at the federal level and removes the ambiguity of allowing each state to dictate individual limitations entirely or forego regulation. Collection events are cleared in advance, and the technology approved for collections is appropriate to the offense perpetrated. The legality of collecting and the authorized scope of the collection are approved based on the evidence presented ahead of time and reviewed by competent federal authority. This solution is most closely aligned with current-day audio and data interception law, and as such, has arguably addressed and assuaged issues surrounding Fourth Amendment rights to privacy.

This solution has limited inherent mechanisms to capture all variants of technology that will be developed in the foreseeable future. Much like the current Title III, today's language to capture surveillance capability will be rendered obsolete over time as technology continues to morph.

2. Feasibility

This solution is feasible. The framework and mechanisms required to update Title III are in place and have been used before to address the changing landscape in the field of technology. The original Title III laws were amended to accommodate the shift from landline-based phone systems to cellular and mobile systems. This law was also modified to allow for the interception of broad forms of data associated with both cellular networks and the internet data transmission platform. Cameras and surveillance systems are

commonplace in society and readily available to all U.S. citizens. Equipping law enforcement agencies and ensuring valid legal mechanisms for creating actionable data for prosecutions is the next logical step to preventing an abuse of power.

E. COUNTERARGUMENTS, CAVEATS, AND ALTERNATIVE INTERPRETATIONS

Regulation at the individual state level may be more appropriate to determine surveillance requirements and limitations. Many states have already established video surveillance laws appropriate to the local environment and will be resistant to federal mandates on an issue already adequately resolved at a lower level.

1. Difficulty Implementing

The resultant benefit of codifying visual surveillance into Title III law will yield a minimal benefit compared to the amount of effort it will take to expand the legislation. It will be challenging to find someone willing to sponsor and champion the change given the pushback from key players, including state government, the ACLU, and the general public against providing a federal mechanism to surveil U.S. citizens on U.S. soil visually.

2. Difficulty Acting On and Obstacles to Execution

The window of opportunity on emergent collection opportunities is short. A thorough federal review of probable cause and other elements necessary to meet Title III requirements will likely prove too lengthy to capitalize on most visual surveillance opportunities.

3. Shortcomings

Assigning long-term ongoing visual surveillance on a specific target is not likely to provide useful information. Drones are easily spotted and thwarted; additionally, they currently have very limited flight profiles in terms of duration. Other surveillance methods are currently superior to drone-based video surveillance for gathering intelligence during extended collects. Drones are best suited to acting as a force multiplier to increase visual coverage areas in short-term applications, for example over protests or demonstrations,

crowd control, and situational tools in advance of special weapons and tactics (SWAT)-style breaches.

F. CONCLUSION

Title III adequately protects against privacy infringement, and its expansion will ensure the safety and security of U.S. citizens are provided at the highest level possible using the most advanced technological means on the market today. A federally mandated limitation framework serves to assuage the fear of the "unknown" when it comes to when and how technology is ultimately employed, as all states and jurisdictions are held to the same constitutionally derived federal standard. Title III expansion to encompass visual surveillance provides a consistent, enforceable legislative framework to place technological advances in law enforcement agents' hands at all levels. The examination of successful uses of facial recognition technology in the daily lives of citizens, studies performed by the ALCU and Amazon, and the outcomes drawn from applicable case law, all support that the responsible use of facial recognition technology by LEOs during active investigations is warranted. The overarching goal of this recommended expansion is to get the available tools into the hands of frontline peace officers.

IV. REGULATING DATA POST-COLLECTION

This chapter examines data regulation after collection events by law enforcement through the creation of new data retention and uses legislation. This chapter discusses six broad recommendations covering the basic outline of responsible data management for law enforcement personnel that include data minimization, redaction, validation, data actionability, retention, and destruction schedules, extension petition procedures, and constitutionally derived external access procedures to ensure Fourth Amendment rights are preserved. PEST analysis identifies major threats and opportunities in the external environment to employing drones effectively in all aspects of the law enforcement mission and also provides relevant data to demonstrate the feasibility of implementing this policy.

Edward Snowden, a former National Security Agency contractor, stated in an interview, "the problem isn't data, the problem is data collection."[88] While many software applications and tools assist in reducing secondary data capture, the lack of data control calls for specifically established measures to prevent infobesity, determine longevity, enable appropriate secondary access and use, control aggregation, establish relevance, define persistence, and answer the question of reasonableness without ambiguity through legislation or body of case law. Data control following collection is fundamental to determining the constitutionality of the collection. Transparency in how the data will be used and by whom is a determinant in protecting privacy.

A. DATA REGULATION POLICY

The most logical course of action for legislators is to adopt data retention and usage policies that minimize unnecessary data storage and control access and dissemination after collection. Legislative policies should establish guidelines for facial recognition-based targeting and non-subject auto-redaction, establish two-party data validation, develop time-limited data actionability, retention, and archival limit schedules, and require federal access

[88] Ryan Browne, "Edward Snowden Says 'the Most Powerful Institutions in Society Have Become the Least Accountable,'" CNBC, November 4, 2019, https://www.cnbc.com/2019/11/04/edward-snowden-warns-about-data-collection-surveillance-at-web-summit.html.

procedures for data otherwise protected under the Constitution, including proving reasonable suspicion or demonstrating probable cause. This recommendation requires the acceptance of five key assumptions regarding surveillance as a discipline: (1) no established federal limits are placed on visual surveillance, (2) visual surveillance enhanced by technological aid (drone, scope, or sensor) is treated as legally equivalent to in-person visual observation, (3) privacy expectations continue to remain at currently reduced levels and will further decline with the mass public acceptance of widely available advanced technological devices, (4) commercial spaces with public access will be treated as public spaces, with no reasonable expectation of privacy during the time the public is reasonably expected to have access to that particular establishment, and (5) in cases where it is in the best interest to the safety of law enforcement personnel or other citizens, visual surveillance methods that provide live visual feedback without data capture are authorized in private domains.

From these key assumptions, legislators should develop a federal framework to steer the regulation and treatment of captured data. All captured surveillance data, regardless of the collection device, should adhere to standardized retention procedures. Six broad recommendations covering the basic outline of responsible data management for law enforcement personnel are as follows:

- Data should be minimized during, or immediately following, collection.[89]
- Non-relevant data not automatically redacted using drone-based software and algorithms should be screened and deleted prior to storage and backup.
- Data deemed relevant to an actionable offense or data-of-interest should be validated by two-party assessment (by agents of two unrelated

89 "29. Electronic Surveillance—Title III Affidavits," Department of Justice Archives, February 19, 2015, https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits.

agencies), then duplicated and archived to protect data integrity and prevent potential tampering.

- Data should be deemed actionable for X years; then, once it has reached the statute of limitations, it should be archived for an additional Y years. Following the period of the archive, the data should be destroyed.

- Data meeting the criteria for an extenuating circumstance requires that a federal court grant a petition for an extension of the archive.

- Data captured by surveillance meeting the criteria for privacy under the Fourth Amendment requires that a federal court grant access to the data and only deem it actionable based on similar criteria and cause to that currently required for issuing warrants.

1. Key Assumption 1: No Federal Limits Placed on Visual Surveillance

Smartphones and other hand-held electronic devices have revolutionized the way the world interacts. According to the Massachusetts Institute of Technology's Technology Review, the smartphone "[reached] 40 percent market saturation in just 2½ years."[90] Smartphones have disrupted and displaced major market segments in such areas as GPS and visual capture (video and images). A true pocket PC, smartphones have acted as a capability-leveler that takes the place of a multitude of high-cost specialty technology devices and replaces them with a ubiquitous tool no bigger than a small notepad. Gone are the days of large VHS cameras lugged around by just a few to special events in a suitcase. High-definition video capture, data storage, and streaming access are nearly universally available baked into even the least-equipped smartphones so prevalent in today's tech-savvy world. Visual surveillance in public spaces is a foregone conclusion. While legislation cannot reasonably stop the world from capturing all media, regulating the use

[90] Casey Phillips, "How Smartphones Revolutionized Society in Less than a Decade," Government Technology, November 20, 2014, https://www.govtech.com/products/How-Smartphones-Revolutionized-Society-in-Less-than-a-Decade.html.

of data after the fact of capture is not yet a lost cause. Data regulation is in its infancy but arguably very necessary to preserve privacy in an increasingly tech-centric future.

2. Key Assumption 2: Tech-Enhanced Visual Surveillance Is Legally Equivalent In-person Visual Observation

In his article on considerations for legislators, Gregory McNeal talks at length about the "demonization" of drones as a technology stemming from a fear of "persistent surveillance."[91] It is easy for organizations like the ACLU to rally support behind privacy concerns when the object of their focus is visible, audible, and instantly recognizable and operating in the immediate vicinity. Drones are relatively new to the scene, having joined the national airspace system only as recently as 2015 when they were incorporated following the FAA Modernization and Reform Act (2012).[92] However, drones are simply a vehicle for positioning a sensor. Calls for regulating drones to tackle the issue of surveillance are about as credible as calls to regulate the feet of the police officers who wear body cams. Regulations restricting drone use as a method to curtail surveillance hold the drone as a platform to a higher constitutional standard than similar, legal methods of surveillance whose validity has been found constitutional through jurisprudence. Drone-based surveillance is akin to any other airborne method and is arguably less capable than other current methods due to the payload and flight duration limitations of current-day UAS.

3. Key Assumption 3: Privacy Expectations Surrounding Technology Today Are Reduced and Declining

In line with key assumption 1, prevailing attitudes surrounding technology have shifted largely to acceptance. People today willingly provide such data as age, gender, preferences, physical location, and others, in exchange for a tailored solution or convenience. On-board GPS and navigation systems track not only present location but also save previous destinations and preferred routing. Dating apps and social media

[91] McNeal, "Drones and Aerial Surveillance."

[92] Federal Aviation Administration, "Fact Sheet—Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)."

accounts collect both information directly input by users and determine associations based on common connections to provide friend or dating suggestions, including providing a user's current physical location information to potential contacts. As evinced by Justice Alito:

> When a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining (crowdsourcing) the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.[93]

Data collected in law enforcement surveillance events under this policy will be redacted and stored under very specific guidelines, which are far more transparent than data collected by other parties. Transparency and consistency in regulation will sway opinions of this policy toward acceptance.

4. Key Assumption 4: Public Access Spaces, to Include Businesses, Are Subject to Surveillance

As touched on earlier, the prevailing theme through much of the relevant jurisprudence is that the expectation of protection from aerial viewing is not reasonable when it is conducted from a lawful public vantage point, either airborne or from an otherwise elevated position. This standard holds true for curtilage, which is far more likely to raise concerns toward privacy infringement than general public space. Businesses conduct operations in and with the public, and the decision to surveil operations should be at the discretion of the business. However, should a business choose to surveil the public, it should have a duty to do so responsibly in full compliance with the current laws, regulations, and in line with a 2015 Presidential Memorandum, which sought to "promote economic competitiveness while safeguarding privacy, civil rights, and civil liberties in

93 *Jones*, 565 U.S. 400 (2012).

domestic use of unmanned aircraft systems."[94] The memorandum outlines expectations of privacy protection in section (a), "to the extent that such collection or use is consistent with and relevant to an authorized purpose;" limiting retention of information containing PII to 180 days, without specific overriding authorization; and preventing dissemination "unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements."[95] Under the last provision, to support law enforcement efforts better inside the 180-day data retention window, law enforcement agents' requests for access to data should be honored by businesses to the maximum practicable extent. Finally, as with all other publicly accessible space, if a police officer wearing a bodycam may lawfully enter the space, a similarly equipped drone should not be held to a higher constitutional standard.

5. Key Assumption 5: In the Best Interest of Safety, no Domain (Public or Private) Is Restricted from Non-recorded Surveillance

In a policy debate mediated by the Urban Institute, Spokane Police Chief Frank Straub discussed, in a scenario of probable domestic violence, how a question of consent, victim advocacy, and police bodycams prompted a change in policy. Chief Straub explained that:

> we changed our policies as a result of some of these discussions. Specifically, around the issue of turning off the cameras when entering someone's private residence (somewhat tied to Washington State's interpretation of the Fourth Amendment and the fact that we are a two-party consent state). During the discussion, a woman in the audience [asked] what I would do if I responded to a domestic violence call and her husband answered the door and told me to turn off the camera while she was in the background asking for the recording to continue. We made the policy change that we would not arbitrarily turn the cameras off but would keep them on unless the victim requested that we turn them off.[96]

---

[94] "Presidential Memorandum: Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," White House, February 15, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[95] White House.

[96] Nancy La Vigne, "Evaluating the Impact of Police Body Cameras," Urban Institute, August 3, 2015, https://www.urban.org/debates/evaluating-impact-police-body-cameras.

When lives are on the line, in the context of privacy versus security, safety should universally win out. Privacy infringement can always be addressed after the fact.

By regulating data following collection, rather than trying to regulate each new advancement in technology, legal protections are able to keep pace with advances in technology. These procedures are in line with the recommended UAS voluntary best practices to address privacy, transparency, and accountability issues related to private and commercial use of UASs agreed upon by major stakeholders in 2016, which was developed at the request of President Barack Obama.[97] Best practices include informing affected persons of UAS use and the collection of data, taking care in the collection and storage of information that identifies a particular person, limiting the use and sharing of such data, securing data that has been collected, and monitoring and complying with the law as it evolves.[98]

Further, in the interest of maintaining consistency in the regulation and operation of UASs, and the safety of the NAS as a whole, the regulation of UAS operations should remain the jurisdiction of the FAA. "Substantial air safety issues are raised when the state or local governments attempt to regulate the operation or flight of aircraft. If one or two municipalities enacted ordinances regulating UAS in the navigable airspace and a significant number of municipalities followed suit, fractionalized control of the navigable airspace could result."[99]

B. PEST ANALYSIS—MAJOR OPPORTUNITIES AND THREATS

This section covers the major opportunities and threats for implementing a data collection and retention framework. Minimizing the collection of non-relevant data, transparency, length of time to retain data, and funding are a few factors that stakeholders consider.

---

[97] White House, "Presidential Memorandum."

[98] Angela Simpson, "Finding Common Ground on UAS," National Telecommunications and Information Administration, May 19, 2016, https://www.ntia.doc.gov/blog/2016/finding-common-ground-uas.

[99] Federal Aviation Administration, "Fact Sheet—Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)."

1. Political Practicality

From a political perspective, standardization through federal regulation makes laws both more consistent between agencies and easier to enforce from a law enforcement perspective. Disparate uses and budgets create a haphazard set of rules and guidelines that vary widely between states or within states at a county or local level as jurisdictions disagree on what and how technology should be allowed. Federal data regulation acts as a consistent baseline for the treatment of data.

On the downside, state regulation can be more easily tailored to fit the needs of programs already in place or designed to meet the needs of individual state's law enforcement drone usage profiles. Federal regulation regarding the treatment of data may make the collection of routine data too time-consuming and costly for small-scale law enforcement outfits to participate.

2. Economic Viability

From an economic perspective, data and information security career fields have seen a sharp uptick in demand for professionals to build networks and security systems to ensure data safety and integrity. As a byproduct of shifting to a data regulation-centric model, skilled jobs will emerge in response to expanding data protections for both surveillance data and other public networks.[100] The rise in requirements to provide data integrity and security in conjunction with drone use will likely expand across all law enforcement data systems.

On the downside, generating the budget or funding lines for new technology and computer systems required to comply with data security and storage requirements may prove to be financially insurmountable. Small budget districts may be required to layoff personnel in exchange for rising data storage costs or may find that maintaining such data systems outweighs the benefit of utilizing drones for even routine law enforcement applications.

---

[100] "Occupational Outlook Handbook: Information Security Analysts, Job Outlook," U.S. Bureau of Labor Statistics, last modified date September 1, 2020, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

3. Socio-Cultural Likelihood of Acceptance

From a socio-cultural perspective, the regulation of data to ensure accountability and transparency was the consensus as a basis for the best approach by the National Telecommunications and Information Administration and other major stakeholders in developing voluntary best practices. Among the best practices were the recommendations to take care of the collection and storage of data, limit the use and sharing of collected data, ensure data security, and comply with the law as it evolves.[101] Although not meant to guide regulatory creation, these best practices are in line with the recommendations put forth in this solution.

On the downside, according to reporting on Pew Research Center, surveys found that "Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age."[102] Between the large-scale data mining operations by the National Security Agency (NSA) and such cybersecurity incidents as the Office of Personnel Management's (OPM's) major data breach (2015) targeting the sensitive information of millions, people are justifiably concerned with the large-scale, long-term massing of data.[103]

4. Technological Feasibility

From a technological perspective, data solutions are advancing rapidly. Such methods as cloud and hybrid cloud computing offer relatively inexpensive data solutions designed to address privacy and network security issues as part of a total data solution. Existing solutions using cloud computing architecture could lessen the burden and massive

---

[101] National Telecommunications and Information Administration, *Voluntary Best Practices*, 5.

[102] Mary Madden and Lee Rainie, "Americans' Attitudes about Privacy, Security and Surveillance," *Pew Research Center: Internet, Science & Tech* (blog), May 20, 2015, https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[103] "Cybersecurity Incidents," U.S. Office of Personnel Management, accessed November 4, 2020, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

technological hurdle of designing a safe, economical solution that allows for expanding data capacity from the ground up.[104]

On the downside, any online forum is at a higher risk of attempts to gain unauthorized access to data in the system. While networking increases the opportunity for interagency sharing, the data is vulnerable to external hack or other malicious attempts to gain access.

C. ADDRESSING CORE CONCERNS

This proposal does not address core concerns 1 or 2 by creating regulations to control visual surveillance. This proposal instead reaches a satisfactory middle ground between privacy and security by enabling all use of available technology to ensure security while protecting privacy rights by the careful treatment of collected data.

This policy adequately meets core concern 3 by proposing specific use guidelines and retention schedules to ensure data is protected and relevant to the issue for which it was collected in conjunction with UAS use by law enforcement agencies.

This policy negates core concern 4, because all forms of surveillance are authorized, with data redaction after collection addressing any and all concerns over privacy that may arise with collected data.

This policy does not specifically address core concern 5, but leaves the discussion surrounding multi-party consent and visual surveillance by LEOs to existing state regulation, which falls outside this proposal's scope. However, any data collected under state rules would receive the same privacy protections as other data collections, as specifically outlined in the proposal.

[104] Steve Walker, "5 Benefits of a Cloud Computing Security Solution," *TB Consulting* (blog), May 20, 2019, https://blog.tbconsulting.com/5-benefits-of-a-cloud-computing-security-solution.

D. TRADEOFFS AND FEASIBILITY

Under a PEST analysis, the macro-environmental factors examined in an environmental scan inform strategic planning processes. In the following section, the pros and cons of implementing a policy to regulate data after collection.

1. Pros and Cons

Law enforcement is freely able to capitalize on technology to enhance job performance and increase the safety of officers and citizens alike. Video surveillance provides for the capture of unbiased data, which may be subsequently used to corroborate events and prosecute crimes. Overt surveillance also acts as a deterrent to crime and an inherent de-escalation tool. When people are under observation, they are more likely to be on their "best behavior."

However, data quality and fidelity are subject to and affected by environmental conditions, technical malfunctions, equipment limitations, weather, and other external factors. Collected data is also subject to corruption during collection, transfer, and storage over time. Although a collection event may be valid, the resulting product may be insufficient or too unreliable to be utilized for its intended prosecution. Overreliance on technology over time may also reduce the skills and abilities of the officers, for example, observation, attention to detail, and recall. Spokane Police Chief Frank Staub cited the time required to redact video footage captured by police-worn body cameras as "approximately 2½ hours per one hour of video/audio."[105] Assuming a similar processing time for other forms of visual capture, processing large amounts of video footage may prove too time-consuming to justify the benefit gained.

2. Feasibility

This recommendation is feasible, as it does not overturn any standing legislation or regulations against the use of video surveillance in public. Public video surveillance is widely, successfully used by criminal organizations and near peers and is a demonstrated

[105] La Vigne, "Evaluating the Impact of Police Body Cameras."

model for success. Data capture, screening, and storage capability exist to the level required to execute this recommendation in the present day.

E. COUNTERARGUMENTS, CAVEATS, AND ALTERNATIVE INTERPRETATIONS

This recommendation brings the United States one step closer to being a surveillance state, where every action is monitored and potentially prosecuted. The NSA has pushed the boundaries of reasonable surveillance with little oversight. COVID has opened the door to tracking people for the "greater good," particularly through cell phone contact tracing and geolocation.[106] Without some form of limits on data collection, eventually, no element of an individual's life will not be captured and sold, despite the best efforts at regulating data.

1. Difficulty Implementing

At all levels, the U.S. government currently lacks the infrastructure and personnel to store, screen, and maintain data in the volume to be collected. A current funding source or budget does not exist to establish or maintain this system over the long haul.

2. Difficulty Acting on and Obstacles to Execution

Screening inherently introduces the bias of the screener on the captured data. Taking data out of the context from which it was recorded and retaining it, in part, threatens the integrity of the data as a whole. Dave McClure, Research Associate, expressed his concerns with the redaction of data, stating, "any redaction of citizen(s) actions—for the sake of protecting their privacy—removes critical context for understanding the officer's actions. Without context, pretty much any instance of an officer physically restraining a suspect is going to look like a case of police brutality."[107] Inherent bias will lead to possible exclusion in cases using the data for prosecution. The data is also highly susceptible to theft. The 21st century has seen numerous major data breaches exposing private

[106] Zak Doffman, "COVID-19 Phone Location Tracking: Yes, It's Happening Now—Here's What You Should Know," Forbes, March 27, 2020, https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/.

[107] La Vigne, "Evaluating the Impact of Police Body Cameras."

information to the public, often for sale with malicious intent. Even systems thought to be secure have suffered damaging hacks and such breaches as the Equifax breach on July 29, 2017, which exposed the sensitive information of more than 143 million people.[108]

3. Shortcomings

This recommendation does not provide a viable mechanism for capturing visual surveillance in areas protected under the Fourth Amendment, even with a warrant or probable cause, because data retention and sharing concerns are not adequately addressed.

F. CONCLUSION

Today, consumers are more willing to submit to an invasion of privacy in exchange for the convenience and benefits gained through technological apps and other niceties of information-age commerce. However, this enthusiasm wanes significantly when technology and its subsequent data collection products are applied to the benefit of law enforcement. Drone surveillance of such major public events as the Boston Marathon requires a persistent period of surveillance over a large number of people, coverage that would capture and preserve a wide range of activity and actions.[109] While actions in public are not covered under the "right to privacy," invariably, events will be held during which coverage may be construed as quasi-legal or in violation of minor law and statutes. Data captured under the pretext of large event crowd control could subsequently be scanned in depth by other agencies with the intent of discovering illicit activity. Without a solid framework for the treatment of collected data, the statute of limitations on gathering and aggregating a behavioral history on a person of interest could stretch out indefinitely.

In this case, it is prudent to limit the ability of technology, based not on its capability to collect, but instead based on the moral responsibility to retain data appropriately and within well-defined limitations. To that end, regulation should focus on the privacy

---

[108] Sara Ashley O'Brien, "Giant Equifax Data Breach: 143 Million People Could Be Affected," CNNMoney, September 7, 2017, https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

[109] McNeal, "Drones and Aerial Surveillance."

concerns of captured data after the fact, regardless of the technology employed during the collection.

The legal process of protecting U.S. citizens is as impressive as it is slow. It is a comprehensive process designed to deliberate and measure carefully to achieve the most just and balanced outcome, but is by nature ill equipped to adapt at the speed of innovation. Data, and how to protect it in the information age, is far better suited to the discussion of protecting privacy. This recommendation's overarching goal is to get the available tools into the hands of frontline patrol to ensure the American society maintains the capability to preserve the safety and security of the United States and its citizens. The United States is behind the power curve with near peers and adversaries who are more than willing to implement technology to their advantage. It will be difficult to maintain a competitive edge into the future as people are overrun by more-capable and better-equipped criminal elements. The time to act is the present, by putting the appropriate technological advances in the hands of law enforcement agents and regulating the collected data on the backside to ensure Fourth Amendment rights are preserved and an abuse of power is prevented. Adopting sound data retention procedures post-collection ensures against privacy infringement and prevents extensive data storage longevity, which may result in the potential for misuse, mishandling, or theft in the future. Regulating data focuses collection on relevance and stops data infobesity in its tracks.

V. RECOMMENDATIONS AND CONCLUSION

A failure to equip state and local law enforcement agents properly can create an asymmetric engagement wherein the balance of power, and the technical advantage, lies with the criminal element. Criminal enterprises in today's society enjoy the full benefits of a technology-rich operating environment created by the free-market availability of COTS equipment. On the other hand, decades-old and obsolete federal surveillance regulations or reactionary overly restrictive and inconsistent state controls provide a daunting obstacle to capitalizing on technology while enforcing U.S. laws and maintaining a safe, well-regulated society.

Each solution represents a sound approach to employing drones effectively in society to increase the safety and security of public spaces within the United States without unduly infringing on the privacy of its citizens. Regulating technology in advance of collection events allows agents specifically to protect privacy and tailor capability to limit the collection of data to only that which is authorized and relevant to a specific crime or action. Conversely, collecting data widely in conjunction with all police action, provides a better context for the data collected, as well as enhancing transparency, accountability, and public trust.

Additionally, both solutions also present some challenges to achieving the goal. Requiring that probable cause and specific evidence be demonstrated prior to visual collection events may specifically preclude capturing the event. Many events that would benefit from corroborative visual surveillance occur and resolve rapidly, and a lengthy authorization time would result in a missed opportunity to gather vital evidence. Similarly, unregulated video surveillance with a nearly unlimited collection of data may serve to provide more data than can be processed and stored, and redaction tied to preserving rights may strip the data of the context required to understand and employ it in prosecuting suspects accurately. In either case, the lack of actionable resulting data makes the cost of implementation and maintenance unconscionable.

A. STAKEHOLDERS

Comparing the major stakeholders' preferences derived from the PEST analysis (Table 2, Appendix B) reveals that the overall consensus is more favorable toward regulation before collection. The prevailing public attitude, though it has shifted away from ultra-privacy in current generations, is still wary of the dangers of becoming an unchecked surveillance state. By requiring that actual evidence and probable cause are both required and vetted through a federal review and requiring minimization, privacy concerns are adequately addressed. Arguably, the public consensus is most likely in line with the proposal of regulation before collection.

Law enforcement recognizes the immense benefit of having drones and other technology available to assist officers in all aspects of the job. Regulation before collection at a federal level is overly complicated and bureaucratic; additionally, it will preclude the ability to apply the necessary technology to all but the most stringently justified circumstances. The majority of the benefit immediately realized from drones and similar technology is in widescale public applications to aid overall situational awareness, for example during protests and rallies, large public events, emergent crowd control requirements, and on-scene accident investigation. This type of employment is best supported by regulation after collection.

The ACLU has come out firmly against recent advances, by citing bias and unreliability in facial recognition technology.[110] Given the inherent bias not only in algorithms programmed to accomplish automatic recognition and the idea of mass surveillance of the public at large, the ACLU would likely be firmly against implementing broad area drone surveillance of all public spaces as a norm. Although regulation before collection provides the inherent mechanisms for protecting against undue infringement of privacy and Fourth Amendment rights, the ACLU is unlikely to support the expansion of Title III due to the inherently invasive nature of the technology in play.

[110] Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots."

The government has important stakeholders at all levels, from local to federal. Expanding Title III to capture visual surveillance allows for greater standardization and broader control over implementation in all 50 states. As it stands today, states have no consensus and very few limitations regulating visual surveillance. Each state is free to implement controls or not. Only about a third of U.S. states require local and state law enforcement agencies to request a warrant prior to performing a search or surveillance with UAS technology.[111] The spectrum of regulations varies. For instance, Oregon prohibits law enforcement from using UAS except when: (1) authorized use upon issuance of warrant (surveil no more than 30 days), (2) written consent, (3) emergency operations, (4) investigations of crimes and accidents, and (5) training.[112] Whereas Wisconsin allows law enforcement agencies to use drones "in a public place or to assist in an active search and rescue operation, to locate an escaped prisoner, to surveil a place or location for the purpose of executing an arrest warrant, or if a law enforcement officer has reasonable suspicion to believe that the use of a drone is necessary to prevent imminent danger to an individual or to prevent [the] imminent destruction of evidence."[113] The federal government would likely lean favorably toward regulation before collection, whereas state and local governments would likely prefer to retain regulation at a lower level. From the standpoint of how society currently operates and the current-day use of visual recording technology by the public, regulation after collection would be the most logical transition toward regulating data without disrupting the status quo.

Businesses become a key stakeholder primarily when discussing the critical assumption that commercial spaces with public access would be treated as public space with no inherent right to prevent surveillance. This assumption is especially critical to the discussion of regulation after collection. Under this solution, drones operating in the public

---

111 911 Security, *U.S. Drone Laws, Overview of Drone Rules and Regulations in USA by States* (Austin, TX: The University of Texas System, 2019), 2, https://www.utsystem.edu/sites/default/files/offices/police/policies/USDroneLaws.pdf.

112 "Chapter 837—Aircraft Operation," Oregon State Legislature, accessed October 20, 2020, https://www.oregonlegislature.gov/bills_laws/ors/ors837.html.

113 "2015 Wisconsin Statutes & Annotations, 175. Miscellaneous Police Provisions. 175.55 Use of Drones Restricted," Justia Law, accessed October 20, 2020, https://law.justia.com/codes/wisconsin/2015/chapter-175/section-175.55.

domain could enter and operate all spaces occupied by the public or spaces in which the public had access for business transactions. The opportunity to catch unrelated infractions in day-to-day business operations and the ability to pass that information off to relevant agencies for prosecution or on request would likely dissuade businesses from supporting the regulation. Although most businesses operate legitimately, by nature of some businesses, they are not in compliance with all laws and requirements at every moment of every day. A recording makes no gray differentiation for "in process," it merely documents compliance or failure. While businesses likely have no opinion on regulation before collection, the consensus would likely be against regulation after collection, instead preferring that law enforcement only enter for surveillance with cause.

A closer examination of the feasibility factors (Table 1, Appendix B) reveals no clearly predominant solution. Regulating technology before collection was overall positive in the political, economic, and technological feasibility categories. Regulation after collection was overall positive in the political, social, and technological categories.[114] From an economic standpoint, expanding Title III regulation is not directly associated with the ongoing costs of manning, training, and equipping law enforcement agents nationwide at all levels of enforcement. Although it is feasible with today's technology and data management methods to achieve the storage infrastructure required for the solution of regulating data after collection, the funding mechanism is not currently identified and would likely result in the loss of manned capability in markets with small budgets. The staggering economic cost of fully implementing regulation after collection makes it inherently less feasible than expanding Title III and implementing regulation before collection.

B. ADDRESSED CONCERNS

Three out of the five core concerns can be fulfilled by addressing the deficiencies in Title III and incorporating a pre-collection subsection to the existing framework.

[114] Sherley Leong, "From Business Analysis to Policy Evaluation: PEST Analysis as a Research Framework of External Macro-Environment," *Evaluation Research Methods* (blog), March 23, 2019, https://evalres.wordpress.com/2019/03/23/from-business-analysis-to-policy-evaluation-pest-analysis-as-a-research-framework-of-external-macro-environment/.

Amendments to Title III allow law enforcement agencies to conduct visual surveillance with drones by providing a mechanism to ensure visual surveillance meets the Fourth Amendment requirements. Additionally, amending Title III standardizes federal regulation under which all states will be held to the same standards of probable cause, and reasonable suspicion before the collection of surveillance data is authorized. By extension, visual surveillance data collected by drones will be held to the same standards applied to other image and video surveillance means (e.g., body-worn cameras). States would be permitted to implement more restrictive policies than Title III; however, none may fail to meet the minimum federal standard.

Similar to the pre-collection solution, a post-collection data regulation option would address concern 3 by providing specific use guidelines and retention schedules to ensure data is protected and relevant to the issue for which it was collected in conjunction with UAS use by law enforcement agencies. Data regulation and retention also provides an opportunity for such redaction technology as geofencing and image distortion applications, to protect citizens captured through secondary data collection while limiting biometric data storage. Unfortunately, data regulation does not prevent the excessive and rogue use of drone-borne sensors that infringe on U.S. citizens' liberty and privacy. Furthermore, a post-collection solution does not deter or prohibit unreasonable searches and seizures, nor does it adequately provide mission-specific transparency.

Regulating technology prior to collection provides the best solution to aiding law enforcement engagement in cases of a specific target, and the data will be captured in areas considered private in line with Fourth Amendment protection. Regulating and controlling data after collection is the most logical solution to addressing video surveillance in public spaces, regardless of the agent or entity capturing the data or the media used in the capture. Overall, the best solution may be found in a combination of both.

C. RECOMMENDATIONS

UASs offer a myriad of benefits to the law enforcement mission, most of which pose no threat to privacy, as the aforementioned examples show. Therefore, creating legislation completely restricting UAVs' use based on the fear of possible privacy

infringement is not warranted. The discussion about protecting liberty and providing security does not have to be a zero-sum game. To that end, the best way to achieve parity in the effective employment of drones by law enforcement agents is a combination of the previous policies, coupled with a healthy dose of old-fashioned respect. Law enforcement agents should capitalize on the diverse multi-mission capability of drones across all aspects of policing. Private spaces should retain the reasonable expectation of the privacy standard, as defined in Justice Harlan's two-part test, wherein an actual subjective expectation of privacy exists, and society is prepared to recognize it as reasonable.[115] In other words, if and when technology is used to see into private spaces, permission must first be sought, and for a good reason. Otherwise, it is a function of "what you see is what you collect." Lastly, data collection and retention should be guided under the spirit of "community policing," working collaboratively with the public and agencies to improve relations and create a safer society for everyone participating in it.[116]

Increased communication and community awareness regarding drone use by law enforcement agencies are critical to finding the middle ground between realizing UAS' benefits and preserving liberty. The following recommended best practices apply to both solutions:

- Build public trust through transparency and accountability practices
- Publicize scrubbed flight logs and data use; tie to positive outcomes (public relations)
- Highlight lesser-known drone missions (event safety, accident investigation, etc.)
- Publicly release captured footage of non-sensitive surveillance actions

115 "Expectation of Privacy," Legal Information Institute, accessed August 10, 2020, https://www.law.cornell.edu/wex/expectation_of_privacy.

116 Community Policing Consortium, *Understanding Community Policing, A Framework for Action* (Washington, DC: Bureau of Justice Assistance Response Center, 1994), 15, https://www.ncjrs.gov/pdffiles/commp.pdf.

Responsible data handling procedures and limitations are a reality of the Information Age. Sound data management practices underpin the success of both of the policy recommendations put forth. Although data management is central to the post-collection data solution, it is inherent in successfully regulating technology application to ensure that the data subsequently collected may be applied for its intended purpose, as evidence in the judiciary process. To that end:

- Collect information with an eye toward eliminating "infobesity" and "analysis paralysis" by redaction and exclusion of non-relevant data.
- Preserve the integrity of data, and set a reasonable limitation schedule for the aggregation, retention, redaction, and destruction of data.
- Only grant access to data with "good cause" or under reasonable constitutional standards criteria.

Increased safety and security throughout society is the win-win achieved through transparency, collaboration, and mutual respect in the law enforcement element's use of UAS in the United States.

Consensual interception falls outside the scope of Title III authorization or data regulation policy, but it is essential to capture in legislation moving forward. "Consensual interception" covers instances where either the LEO or agent is a party to a conversation or one of any of the parties involved in a conversation gives consent to being monitored, or when there is no justifiable expectation of privacy. Consent to visual surveillance varies greatly as to the requirements from state to state, and not all states have enacted laws concerning visual surveillance. Consistent consensual monitoring exceptions would enable law enforcement elements to capitalize on such technology as the follow-me tracking and facial recognition software to identify and escort people on request in situations where they felt threatened, for example, on college campuses at night or through neighborhoods with a history of opportunistic crime. In departments where manning is critical, having an escort that can follow, geolocate, and alert authorities is an invaluable force multiplier. As discussed earlier in this thesis, a framework consistent across all states that will expand

consensual interception to visual surveillance opens the door for the extension of surveillance as a safety measure or victim advocate.

D. CONCLUSION

Providing a regulated and appropriate physical presence (man or machine) is necessary to deter and stop criminal activity and ensure U.S. citizens' safety and security. Surveillance data collected by drone-borne sensors furthers that goal. The original question asks whether domestic law enforcement agencies should expand their jurisdiction to provide protection and intelligence collection via the use of UAS within U.S. borders. Present-day drone operations at U.S. borders and overseas have demonstrated the powerful advantage gained by using aerial surveillance sensors. It is less of a question of "whether" an advantage is gained, but more realistically of "how" to minimize the collateral impact on privacy rights and civil liberties.

Law enforcement drones significantly improve the enforcement agencies' ability to counter groups and factions conducting illicit activities to harm the United States, its infrastructure, and its citizens. Nefarious organizations, internal and external to U.S. interests, are willing and able to exploit any technological advantage to achieve their goals, and as a nation of law-abiding citizens, U.S. citizens must stand ready to do the same. While inherent vulnerabilities exist in the use of UAVs, implementing reasoned control measures, training, and oversight when wielding UAV technology will garner support from the general public and allow law enforcement agencies (state, local, and federal) to continue to gather intelligence and counter these threats more effectively. For uses that may be considered riskier to constitutionally derived reasonable expectations of privacy, or even in cases not protected but meeting the second part of the Katz test, law enforcement agents can be trained to err on the side of demonstrating probable cause and reasonable suspicion.

Moreover, drones offer many valuable benefits not targeted at deterring crime. In light of recent technological advances, state and local law enforcement agencies can and should employ drones in society. Public safety missions, for example search and rescue, on-scene traffic accident investigation, or assessing crowds in such volatile situations as

riots or protests all help increase the safety and security of public spaces without infringing on the privacy of U.S. citizens. Natural disaster response and recovery efforts are also significantly aided by using small UASs to locate victims, deliver supplies, and act as ad-hoc communications networks to carry signals to remote areas or bridge non-coverage zones. Future programs, like the proposed "Follow Me" campus security model, or similar programs with drones escorting people through risky neighborhoods upon request, are made possible by ensuring that technology is not unnecessarily limited out of fear or broader political agenda.

Thus, what comes next depends mostly on the collective wisdom and collaborative nature of the key players in the debate. This thesis attempts to highlight the distinction between surveillance technology and delivery platforms to understand how to approach regulating data gathering better. In doing so, this thesis examined Title III and relative jurisprudence dealing with both surveillance and aerial platforms to bring forward the salient points in crafting recommendations that support an increase in citizens' safety and security but remain within the bounds of constitutional liberty and the Fourth Amendment. To that end, the best way to achieve that goal is to develop a framework to regulate data.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. POLITICAL, ECONOMIC, SOCIAL, TECHNOLOGICAL (PEST) ANALYSIS

POLITICAL

- Visual surveillance is not federally regulated and is inconsistent between states (-)
- Lack of federal regulation allows for easier implementation of programs at the local level (+)
- Title 10/ 14 jurisdiction issues cloud consensus on who wields tech and shares info (-)
    - Concerns surrounding surveilling U.S. citizens on U.S. soil
    - 100-mile gray zone
- Possibility of federal taxes used to subsidize safety surveillance program (-)
- Standardization through regulation makes laws easier to enforce (+)
- Regulation provides clear guidance for states to follow (+)
- Solutions capture the possibility of future growth/innovation without additional expansion needed to regulations at each successive iteration (+)
- Competitors/near peers/nefarious elements already have access to an utilize technological advancements to gain an advantage (-)
- Regulation expansion can draw from existing expertise in FAA UAS implementation (+)

ECONOMIC

- Successful UAS implementation requires long term funding (-)
    - Technology repairs and upgrades (-)
    - Equipment loss (-)
    - Training/proficiency (-)
    - Tax increase or other budget tradeoff (-)
- Small UAS systems are cheaper to obtain/own/operate than the manned equivalent (+)
- Low cost Commercial Off The Shelf (COTS) (+)
    - Wide availability
    - Affordable
    - Small benefit
- Any additional cost to small budget districts may result in layoffs (-)
- Technology quality is an inherent tradeoff with price point (+/-)
    - Higher availability/lower cost (+)
    - Lower quality/reliability (-)
    - Fewer features/less capability (-)
- Increased cost to protect businesses with surveillance (-)
    - Licensing
    - Certification
    - Cooperation with information sharing requests

- Current economy is struggling; opportunity for new growth in market (+)
- Wide market for tech training and research opportunities (+)

SOCIAL

- Drone operations are viewed as more intrusive and suspicious than physical presence (-)
- Expectation of privacy tradeoff (+/-)
  - People are able to use technology to enhance their lives (+)
  - Enhancements require increasing amounts of data about people to work (-)
- Fosters unrealistic public expectations (-)
  - Capability
  - Coverage
  - Fidelity
  - Actionability of data collected
- Enhances safety of LEO and civilians entering dangerous/unknown situations (+)
- Potential to degrade LEO skills if officers become too complacent/reliant on tech (-)
- Tech loss of control can endanger crowds or violate airspace; safety and disruption (-)
- Drone transit can be seen as a nuisance (-)
- Drone delivery service increases positive public perception (+)
- Drone presence enhances crowd control (+/-)
  - People less likely to escalate situations under observation (+)
  - Eyes on without a physical presence (+)
  - Better area coverage; one person can monitor many drones (+)
  - Slower response time; physical presence is not on-site (-)
- People have not actively consented to being monitored/recorded (-)
- Public currently has a negative attitude associated with NSA surveillance (-)
- Streamline prosecution and chain of evidence (+)
- Business may resent government interference in monitoring self (-)
- Clientele may be affected by LEO linked surveillance in businesses (+/-)
- U.S. is currently in a climate of unrest; non-confrontational law enhancement tool (+)
  - Non-intrusive increase in coverage of volatile situations
  - Force multiplier
- Global presence: visual surveillance systems successfully operate throughout the world (+)
  - Similar countries
  - Demonstrated model for success/public acceptance
- Boomer generation is dying, shifting the prevailing attitude towards tech-positive (+)
  - Current/future generations grew up with tech (+)
  - Privacy expectations of current/future generation tempered by desire for tech (+)
  - Current/future gen. highly educated, less susceptible to ignorance-based fear and misinformation (+)

- Large influential companies (Amazon/Walmart/UPS) embracing drones in operations (+)
    - Drone use associated with positive connotations
        - Mail delivery/medical supplies
        - Wedding and event videography
        - Food delivery
    - Increases public comfort levels and acceptance of drone operations
- Large market shift toward autonomy (+)
    - Drone-assisted retail
    - Unmanned vehicles
    - Car autopilot assist
    - Camera-intensive applications
- Media/propaganda less likely to drive agendas; independent verification dispels spin (+)

TECHNOLOGICAL

- New technology is inherently more capable, giving users an increased advantage over unassisted methods and/or previous generations of similar technology (+)
- Increases in technology generally produce faster results or increase efficiency (+)
- Drone-based visual surveillance allows a physical standoff from potentially dangerous or unstable situations without losing situational awareness (+)
- Drone sensors can record on the fly, creating a reliable and unbiased record of events (+)
- Provide access beyond human capability in difficult terrain/extreme conditions (+)
    - Deliver supplies (+)
    - Assess conditions (+)
    - Establish remote communications (+)
- Drone/tech subject to loss of control (-)
    - Spoofing
    - Insufficient training
    - Tech failure
- Identification via algorithm not currently reliable/ demonstrates a programmer bias (-)
- False positive identification possible due to system limitations/degradation (-)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PEST ANALYSIS RESULTS—STAKEHOLDER PREFERENCE AND FEASIBILITY TABLES

Table 1. Pest Feasibility Chart

OPTIONS				
Regulation before Collection	+	+	-	+
Regulation after Collection	+	-	+	+
CRITERIA	**POLITICAL FEASIBILITY**	**ECONOMIC FACTORS**	**SOCIAL FACTORS**	**TECHNOLOGICAL FEASIBILITY**

Determines which option predominates in each category to make a clear recommendation

Table 2. Stakeholder Preference

OPTIONS					
Regulation before Collection	+	-	-	+	+
Regulation after Collection	-	+	-	+	-
CRITERIA	**The Public**	**Law Enforcement**	**ACLU/ Similar**	**Government**	**Business**

Determines the stakeholder preference; prioritizes the recommendation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

911 Security. *U.S. Drone Laws, Overview of Drone Rules and Regulations in USA by States*. Austin, TX: The University of Texas System, 2019. https://www.utsystem.edu/sites/default/files/offices/police/policies/USDroneLaws.pdf.

American Civil Liberties Union. "Big Data." Accessed November 23, 2020. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/big-data.

———. "Domestic Drones." Accessed June 5, 2020. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

———. "What's Wrong with Public Video Surveillance?." March 2002. https://www.aclu.org/other/whats-wrong-public-video-surveillance.

Anderson, Janna, and Lee Rainie. "Stories from Experts about the Impact of Digital Life, 3. Fifty-fifty Anecdotes: How Digital Life Has Been both Positive and Negative." *Pew Research Center: Internet, Science & Tech* (blog). July 3, 2018. https://www.pewresearch.org/internet/2018/07/03/fifty-fifty-anecdotes-how-digital-life-has-been-both-positive-and-negative/.

Browne, Ryan. "Edward Snowden Says 'The Most Powerful Institutions in Society Have Become the Least Accountable.'" CNBC, November 4, 2019. https://www.cnbc.com/2019/11/04/edward-snowden-warns-about-data-collection-surveillance-at-web-summit.html.

Busch, Michel. "Unmanned Aerial Systems Miniaturization." *Joint Air Power Competence Centre* (blog). March 22, 2018. https://www.japcc.org/unmanned-aerial-systems-miniaturization/.

Community Policing Consortium. *Understanding Community Policing, A Framework for Action*. Washington, DC: Bureau of Justice Assistance Response Center, 1994. https://www.ncjrs.gov/pdffiles/commp.pdf.

Corrigan, Fintan. "12 Best Follow Me Drones and Follow You Technology Reviewed." DroneZon, October 18, 2020. https://www.dronezon.com/drone-reviews/best-follow-me-gps-mode-drone-technology-reviewed/.

Crudo, Timothy, and Nicholas Lin. *Wiretapping for Beginners*. New York: Law360, 2011. https://m.lw.com/thoughtLeadership/wiretapping-basics.

Defense Privacy and Civil Liberties Office. *Introduction to The Privacy Act*. Arlington, VA: Defense Privacy and Civil Liberties Office, n.d. Accessed November 18, 2020. https://dpcld.defense.gov/Portals/49/Documents/Privacy/2011%20DPCLO_Intro_Privacy_Act.pdf.

Department of Homeland Security. "Snapshot: First Responders Assess Drones for Search and Rescue Missions." April 2, 2020. https://www.dhs.gov/science-and-technology/news/2020/04/02/snapshot-first-responders-assess-drones-search-and-rescue-missions.

Department of Justice. "9-7.000—Electronic Surveillance." February 19, 2015. https://www.justice.gov/jm/jm-9-7000-electronic-surveillance.

Department of Justice Archives. "28. Electronic Surveillance—Title III Applications." February 19, 2015. https://www.justice.gov/archives/jm/criminal-resource-manual-28-electronic-surveillance-title-iii-applications.

———. "29. Electronic Surveillance—Title III Affidavits." February 19, 2015. https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits.

———. "32. Video Surveillance—Use of Closed-Circuit Television (CCTV)." February 19, 2015. https://www.justice.gov/archives/jm/criminal-resource-manual-32-video-surveillance-use-closed-circuit-television-cctv.

Doffman, Zak. "COVID-19 Phone Location Tracking: Yes, It's Happening Now—Here's What You Should Know." Forbes, March 27, 2020. https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/.

Electronic Privacy Information Center. "United States v. Jones." Accessed November 11, 2020. https://epic.org/amicus/jones/.

Federal Aviation Administration. "Fact Sheet—Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)." October 6, 2020. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615.

Figliola, Patricia Moloney. *Digital Surveillance: The Communications Assistance for Law Enforcement Act*. CRS Report No. RL30677. Washington, DC: Congressional Research Service, 2007. https://fas.org/sgp/crs/intel/RL30677.pdf.

Findlaw. "FindLaw's United States Supreme Court Case and Opinions." Accessed November 4, 2020. https://caselaw.findlaw.com/us-supreme-court/328/256.html.

Fishman, Clifford S. “Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice.” *Georgia Law Review* 22, no. 1 (1987): 1–89. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1506&context=scholar.

Fordham University. “Conducting an Environmental Scan.” Accessed November 4, 2020. https://www.fordham.edu/info/26625/conducting_an_environmental_scan#.

Guariglia, Matthew. “How to Identify Visible (and Invisible) Surveillance at Protests.” Electronic Frontier Foundation, June 4, 2020. https://www.eff.org/deeplinks/2020/06/how-identify-visible-and-invisible-surveillance-protests.

Harmacinski, Jill. “Eyes in the Sky: Drones a ‘Force Multiplier’ for Lawrence Police Department.” *The Eagle Tribune*, October 17, 2020. https://www.eagletribune.com/news/merrimack_valley/eyes-in-the-sky-drones-a-force-multiplier-for-lawrence-police-department/article_f128491f-a33f-5aaf-ac9c-47743aa16ac2.html.

History com Editors. “Patriot Act.” History, December 19, 2017. https://www.history.com/topics/21st-century/patriot-act.

Jarmanning, Ally. “Boston Bans Use of Facial Recognition Technology. It’s the 2nd-Largest City to Do So.” WBUR News. Updated June 24, 2020. https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban.

Justia Law. “2015 Wisconsin Statutes & Annotations, 175. Miscellaneous Police Provisions. 175.55 Use of Drones Restricted.” Accessed October 20, 2020. https://law.justia.com/codes/wisconsin/2015/chapter-175/section-175.55.

Justice Information Sharing. “Title III of The Omnibus Crime Control and Safe Streets Act of 1968.” Accessed October 20, 2020. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.

La Vigne, Nancy. “Evaluating the Impact of Police Body Cameras.” Urban Institute, August 3, 2015. https://www.urban.org/debates/evaluating-impact-police-body-cameras.

Legal Information Institute. “18 U.S. Code § 2511—Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.” Accessed October 20, 2020. https://www.law.cornell.edu/uscode/text/18/2511.

———. “18 U.S. Code § 2518—Procedure for Interception of Wire, Oral, or Electronic Communications.” Accessed August 10, 2020. https://www.law.cornell.edu/uscode/text/18/2518.

———. “18 U.S. Code Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications.” Accessed August 10, 2020. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

———. “Exclusionary Rule.” Accessed November 11, 2020. https://www.law.cornell.edu/wex/exclusionary_rule.

———. “Expectation of Privacy.” Accessed August 10, 2020. https://www.law.cornell.edu/wex/expectation_of_privacy.

———. “Fourth Amendment.” Accessed February 24, 2020. https://www.law.cornell.edu/wex/fourth_amendment.

Leong, Sherley. “From Business Analysis to Policy Evaluation: PEST Analysis as a Research Framework of External Macro-Environment.” *Evaluation Research Methods* (blog). March 23, 2019. https://evalres.wordpress.com/2019/03/23/from-business-analysis-to-policy-evaluation-pest-analysis-as-a-research-framework-of-external-macro-environment/.

Madden, Mary, and Lee Rainie. “Americans’ Attitudes about Privacy, Security and Surveillance.” *Pew Research Center: Internet, Science & Tech* (blog). May 20, 2015. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

McNeal, Gregory. “Drones and Aerial Surveillance: Considerations for Legislatures.” *Brookings* (blog). November 13, 2014. https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/.

National Telecommunications and Information Administration. *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability Consensus, Stakeholder-Drafted Best Practices Created in the NTIA-Convened Multistakeholder Process*. Washington, DC: National Telecommunications and Information Administration, 2016. https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

O’Brien, Sara Ashley. “Giant Equifax Data Breach: 143 Million People Could Be Affected.” CNNMoney, September 7, 2017. https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

Oregon State Legislature, Chapter 837—Aircraft Operation.” Accessed October 20, 2020. https://www.oregonlegislature.gov/bills_laws/ors/ors837.html.

Oyez. “California v. Ciraolo.” Accessed March 8, 2020. https://www.oyez.org/cases/1985/84-1513.

———. “Dow Chemical Company v. United States.” Accessed March 8, 2020. https://www.oyez.org/cases/1985/84-1259.

———. “Katz v. United States.” Accessed November 11, 2020. https://www.oyez.org/cases/1967/35.

———. “Olmstead v. United States.” Accessed December 3, 2020. https://www.oyez.org/cases/1900-1940/277us438.

———. “United States v. Causby.” Accessed November 11, 2020. https://www.oyez.org/cases/1940-1955/328us256.

Phillips, Casey. “How Smartphones Revolutionized Society in Less than a Decade.” Government Technology, November 20, 2014. https://www.govtech.com/products/How-Smartphones-Revolutionized-Society-in-Less-than-a-Decade.html.

Pookkottuvariam, Niveditha. “Future of Moore’s, Kryder’s, and Robert’s Laws.” Medium, January 26, 2019. https://medium.com/@nivedithaartist/future-of-moores-kryder-s-and-robert-s-laws-27c79ef343a8.

Prieve, Judith. “Bay Area Police Agencies Say Drones Are a ‘Force Multiplier.’” July 22, 2019. https://www.govtech.com/public-safety/Bay-Area-Police-Agencies-Say-Drones-Are-a-Force-Multiplier.html.

Rall, Ted. “The Pros and Cons of Facial Recognition; Debate Safety and Civil Liberties before it Becomes Ubiquitous.” *Wall Street Journal*, May 2019. Proquest.

Rodriguez, Nancy, Howard Spivak, Chris Tillery, Mark Greene, and Michael O’Shea. *Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program*. NCJ 250283. Washington, DC: National Institute of Justice, 2016. https://www.ncjrs.gov/pdffiles1/nij/250283.pdf.

Sands, Geneva. “Customs and Border Protection Drone Flew over Minneapolis to Provide Live Video to Law Enforcement.” CNN, May 29, 2020. https://www.cnn.com/2020/05/29/politics/cbp-drone-minneapolis/index.html.

Simpson, Angela. “Finding Common Ground on UAS.” National Telecommunications and Information Administration, May 19, 2016. https://www.ntia.doc.gov/blog/2016/finding-common-ground-uas.

Slobogin, Christopher. “Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity.” *Mississippi Law Journal* 72 (2002): 213–315. doi:http://dx.doi.org/10.2139/ssrn.364600.

Snow, Jacob. “Amazon’s Disturbing Plan to Add Face Surveillance to Your Front Door.” American Civil Liberties Union, December 12, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-your.

———. “Amazon’s Face Recognition Falsely Matched 28 Members of Congress with Mugshots.” *ALCU* (blog). July 26, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

Society for Computers and Law. “High Court Dismisses Claim for Judicial Review in Facial Recognition Technology Case: Bridges and Another v South Wales Police.” September 4, 2019. https://www.scl.org/news/10656-high-court-dismisses-claim-for-judicial-review-in-facial-recognition-technology-case-bridges-and-another-v-south-wales-police.

Stanley, Jay. “Protests, Aerial Surveillance, and Police Defunding.” American Civil Liberties Union, June 24, 2020. https://www.aclu.org/news/national-security/protests-aerial-surveillance-and-police-defunding/.

Tom’s Tech Time. “DJI ActiveTrack Mode Explained.” Accessed November 4, 2020. https://www.tomstechtime.com/active-track-mode.

U.S. Bureau of Labor Statistics. “Occupational Outlook Handbook: Information Security Analysts, Job Outlook.” Last modified date September 1, 2020. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

U.S. Customs and Border Protection. “Eagle Pass CBP Officers Seize over $300K of Narcotics at Port.” January 23, 2017. https://www.cbp.gov/newsroom/local-media-release/eagle-pass-cbp-officers-seize-over-300k-narcotics-port.

U.S. Office of Personnel Management. “Cybersecurity Incidents.” Accessed November 4, 2020. https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

UpCounsel. “Video Surveillance Laws by State: Everything You Need to Know.” Accessed August 10, 2020. https://www.upcounsel.com/video-surveillance-laws-by-state.

Valdovinos, Maria, James Specht, and Jennifer Zeunik. *Community Policing & Unmanned Aircraft Systems (UAS): Guidelines to Enhance Community Trust*. Washington, DC: Office of Community Oriented Policing Services, 2016. https://rems.ed.gov/docs/COPS_Community-Policing-UAS.pdf.

Valley, Jackie. “You’re Being Watched: Inside Las Vegas’ Surveillance Culture.” *Las Vegas Sun*, October 5, 2014. https://lasvegassun.com/youre-being-watched/.

Walker, Steve. “5 Benefits of a Cloud Computing Security Solution.” *TB Consulting* (blog). May 20, 2019. https://blog.tbconsulting.com/5-benefits-of-a-cloud-computing-security-solution.

White House. “Presidential Memorandum: Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.” February 15, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

Wired. “The FBI Wanted a Backdoor to the IPhone. Tim Cook Said No.” Accessed November 11, 2020. https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

Wood, Matt. “Thoughts on Machine Learning Accuracy.” *AWS News* (blog). July 27, 2018. https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/?tag=theverge02-20.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California